PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-163661
(43)Date of publication of application : 06.06.2003

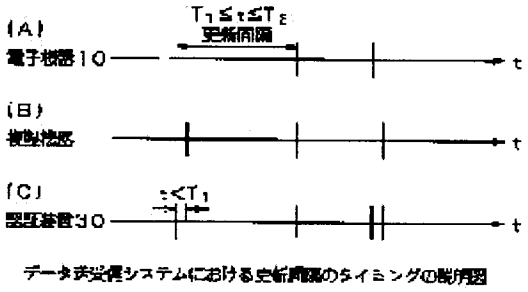
(51)Int.Cl. H04L 9/10
G09C 1/00
H04L 9/32

(21)Application number : 2001-361032
(22)Date of filing : 27.11.2001

(71)Applicant : SONY CORP
(72)Inventor : SAITO SHINYA

(54) ELECTRONIC EQUIPMENT, AUTHENTICATION DEVICE, AND SYSTEM AND METHOD FOR DETECTING DUPLICATION EQUIPMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To detect the existence of duplication equipment by tracing the duplication equipment.
SOLUTION: In a data transmission and reception system, even when proper electronic equipment 10 informs an authentication device 30 of a request for update always at prescribed intervals with a range T1≤t≤T2 as shown in (A), and the duplication equipment informs the authentication device 30 of the request for update at the same intervals as the update intervals of the electronic equipment 10 as shown in (B), a difference is produced between a time when the information of the request reaches the authentication device 30 from the electronic equipment 10 and is accepted and a time when the information of the request reaches the authentication device 30 from the duplication equipment and is accepted. Then, intervals of reaching of the information of the request to the authentication device 30 is deviated from the prescribed range T1≤t≤T2 as shown in (C). By taking notice of the deviation and inspecting the compatibility of the updating intervals of key data, the connected duplicating equipment is traced to detect the existence of the duplicated equipment.



データ送受信システムにおける更新間隔のタイミングの説明図

LEGAL STATUS

[Date of request for examination] 29.11.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

4

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－163661
（P2003－163661A）
(43)公開日　平成15年６月６日(2003.6.6)

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ　9/10		Ｇ０９Ｃ　1/00	６４０Ｅ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０	Ｈ０４Ｌ　9/00	６２１Ａ	
Ｈ０４Ｌ　9/32			６７５Ｄ	
			６７５Ｂ	

審査請求　未請求　請求項の数32　ＯＬ　（全 27 頁）

(21)出願番号　特願2001－361032(P2001－361032)

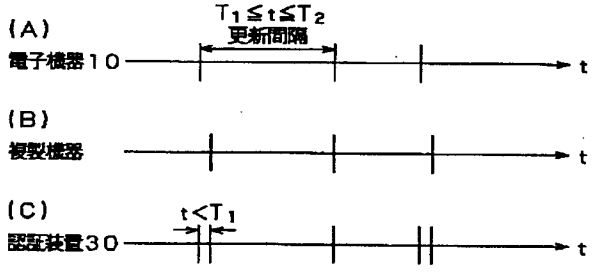
(22)出願日　平成13年11月27日(2001.11.27)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　齊藤　真也
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100110434
弁理士　佐藤　勝

Ｆターム(参考)　5J104 AA07 AA44 EA19 JA21 KA02 KA05

(54)【発明の名称】　電子機器及び認証装置、並びに複製機器検出システム及び複製機器検出方法

(57)【要約】
【課題】　複製機器を追跡し、複製機器の存在を検出する。
【解決手段】　データ送受信システムにおいては、（Ａ）に示すように、正当な電子機器１０が常に所定の範囲Ｔ１≦ｔ≦Ｔ２の間隔で、更新のリクエストを認証装置３０に対して通知し、（Ｂ）に示すように、複製機器が電子機器１０の更新間隔と同間隔で、更新のリクエストを認証装置３０に対して通知する場合であっても、電子機器１０から認証装置３０に対してリクエストの通知が到達して受諾される時刻と、複製機器から認証装置３０に対してリクエストの通知が到達して受諾される時刻との間に差が生じ、認証装置３０に対してリクエストの通知が到達する間隔が、（Ｃ）に示すように、所定の範囲Ｔ１≦ｔ≦Ｔ２から外れることに着目し、鍵データの更新間隔の整合性の検証を行うことにより、接続された複製機器を追跡し、複製機器の存在を検出する。



データ送受信システムにおける更新間隔のタイミングの説明図

【特許請求の範囲】
【請求項１】　正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する電子機器であって、
公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、
最後に公開鍵データを更新した時刻を示す更新時刻情報を上記認証装置から取得する取得手段と、
現在時刻を示す現在時刻情報と、上記取得手段によって取得した上記更新時刻情報と、上記乱数発生手段によって前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えることを特徴とする電子機器。
【請求項２】　上記乱数発生手段によって発生した上記乱数値を、次回の公開鍵データの更新までの時間として記憶する記憶手段を備えることを特徴とする請求項１記載の電子機器。
【請求項３】　公開鍵暗号方式における復号を行う復号手段を備え、
上記取得手段は、上記認証装置によって上記更新時刻情報が暗号化された暗号化更新時刻情報を取得し、
上記復号手段は、上記暗号化更新時刻情報を復号し、上記更新時刻情報を得ることを特徴とする請求項１記載の電子機器。
【請求項４】　上記暗号化更新時刻情報に対する上記認証装置の電子署名の検証を行い、上記暗号化更新時刻情報の検証を行う更新時刻情報検証手段を備えることを特徴とする請求項３記載の電子機器。
【請求項５】　上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が不当なものであると判定された場合に、警告としての暗号化更新時刻情報エラーを示す制御信号を上記認証装置に対して送信する送信手段を備えることを特徴とする請求項４記載の電子機器。
【請求項６】　上記更新間隔検証手段は、上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が正当なものであると判定された場合に、上記公開鍵データの更新間隔の整合性の検証を行うことを特徴とする請求項４記載の電子機器。
【請求項７】　上記更新間隔検証手段による検証の結果、上記複製機器が存在していないものと判定された場合には、上記公開鍵データの更新処理を行うことを特徴とする請求項１記載の電子機器。
【請求項８】　上記更新間隔検証手段による検証の結果、上記複製機器が存在しているものと判定された場合には、警告を発することを特徴とする請求項１記載の電子機器。
【請求項９】　公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置であって、
所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、
上記更新間隔検証手段による検証の結果に応じた検証結果情報を上記電子機器に対して送信する送信手段とを備えることを特徴とする認証装置。
【請求項１０】　上記検証結果情報を上記正当な電子機器の公開鍵データを用いて暗号化する暗号化手段を備え、
上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報を上記電子機器に対して送信することを特徴とする請求項９記載の認証装置。
【請求項１１】　上記認証機関の秘密鍵データを用いて上記検証結果情報の電子署名を生成する電子署名生成手段を備え、
上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報と上記電子署名とを上記電子機器に対して送信することを特徴とする請求項１０記載の認証装置。
【請求項１２】　上記送信手段は、上記更新間隔検証手段による検証の結果、上記差分が上記所定の範囲内にないものと判定された場合には、上記検証結果情報として、上記更新リクエストを拒否する旨を示す警告情報を上記電子機器に対して送信することを特徴とする請求項９記載の認証装置。
【請求項１３】　上記送信手段は、上記更新間隔検証手段による検証の結果、上記差分が上記所定の範囲内にあるものと判定された場合には、上記検証結果情報として、上記更新リクエストを受諾する旨を示す受諾情報を上記電子機器に対して送信することを特徴とする請求項９記載の認証装置。
【請求項１４】　正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、
上記電子機器は、
公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置

に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、
最後に公開鍵データを更新した時刻を示す更新時刻情報を上記認証装置から取得する取得手段と、
現在時刻を示す現在時刻情報と、上記取得手段によって取得した上記更新時刻情報と、上記乱数発生手段によって前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えることを特徴とする複製機器検出システム。
【請求項１５】　上記電子機器は、上記乱数発生手段によって発生した上記乱数値を、次回の公開鍵データの更新までの時間として記憶する記憶手段を備えることを特徴とする請求項１４記載の複製機器検出システム。
【請求項１６】　上記認証装置は、
上記更新時刻情報を上記正当な電子機器の公開鍵データを用いて暗号化する暗号化手段と、
上記暗号化手段によって生成された暗号化更新時刻情報を上記電子機器に対して送信する送信手段とを備えることを特徴とする請求項１４記載の複製機器検出システム。
【請求項１７】　上記電子機器は、公開鍵暗号方式における復号を行う復号手段を備え、
上記取得手段は、上記認証装置における上記暗号化手段によって生成された上記暗号化更新時刻情報を取得し、
上記復号手段は、上記暗号化更新時刻情報を復号し、上記更新時刻情報を得ることを特徴とする請求項１６記載の複製機器検出システム。
【請求項１８】　上記認証装置は、上記認証機関の秘密鍵データを用いて上記暗号化更新時刻情報の電子署名を生成する電子署名生成手段を備え、
上記送信手段は、上記暗号化更新時刻情報と上記電子署名とを上記電子機器に対して送信することを特徴とする請求項１７記載の複製機器検出システム。
【請求項１９】　上記電子機器は、上記暗号化更新時刻情報に対する上記電子署名の検証を行い、上記暗号化更新時刻情報の検証を行う更新時刻情報検証手段を備えることを特徴とする請求項１８記載の複製機器検出システム。
【請求項２０】　上記電子機器は、上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が不当なものであると判定された場合に、警告としての暗号化更新時刻情報エラーを示す制御信号を上記認証装置に対して送信する他の送信手段を備えることを特徴とする請求項１９記載の複製機器検出システム。
【請求項２１】　上記更新間隔検証手段は、上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が正当なものであると判定された場合に、上記公開鍵データの更新間隔の整合性の検証を行うことを特徴とする請求項１９記載の複製機器検出システム。
【請求項２２】　上記電子機器は、上記更新間隔検証手段による検証の結果、上記複製機器が存在していないものと判定された場合には、上記公開鍵データの更新処理を行うことを特徴とする請求項１４記載の複製機器検出システム。
【請求項２３】　上記電子機器は、上記更新間隔検証手段による検証の結果、上記複製機器が存在しているものと判定された場合には、警告を発することを特徴とする請求項１４記載の複製機器検出システム。
【請求項２４】　正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、
公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する上記電子機器による公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を上記電子機器によって発生する乱数発生工程と、
最後に公開鍵データを更新した時刻を示す更新時刻情報を上記電子機器によって上記認証装置から取得する取得工程と、
現在時刻を示す現在時刻情報と、上記取得工程にて取得した上記更新時刻情報と、上記乱数発生工程にて前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記電子機器によって上記公開鍵データの更新間隔の整合性を検証する更新間隔検証工程とを備えることを特徴とする複製機器検出方法。
【請求項２５】　正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、
公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置は、
所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、
上記更新間隔検証手段による検証の結果に応じた検証結果情報を上記電子機器に対して送信する送信手段とを備えることを特徴とする複製機器検出システム。

【請求項２６】　上記認証装置は、上記検証結果情報を上記正当な電子機器の公開鍵データを用いて暗号化する暗号化手段を備え、
上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報を上記電子機器に対して送信することを特徴とする請求項２５記載の複製機器検出システム。
【請求項２７】　上記電子機器は、
上記暗号化手段によって暗号化された上記検証結果情報を上記認証装置から取得する取得手段と、
公開鍵暗号方式における復号を行う復号手段とを備え、
上記復号手段は、上記取得手段によって取得した暗号化された上記検証結果情報を復号し、上記検証結果情報を得ることを特徴とする請求項２６記載の複製機器検出システム。
【請求項２８】　上記認証装置は、上記認証機関の秘密鍵データを用いて上記検証結果情報の電子署名を生成する電子署名生成手段を備え、
上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報と上記電子署名とを上記電子機器に対して送信することを特徴とする請求項２７記載の複製機器検出システム。
【請求項２９】　上記電子機器は、上記検証結果情報に対する上記電子署名の検証を行い、上記検証結果情報の検証を行う検証結果情報検証手段を備えることを特徴とする請求項２８記載の複製機器検出システム。
【請求項３０】　上記送信手段は、上記更新間隔検証手段による検証の結果、上記差分が上記所定の範囲内にないものと判定された場合には、上記検証結果情報として、上記更新リクエストを拒否する旨を示す警告情報を上記電子機器に対して送信することを特徴とする請求項２５記載の複製機器検出システム。
【請求項３１】　上記送信手段は、上記更新間隔検証手段による検証の結果、上記差分が上記所定の範囲内にあるものと判定された場合には、上記検証結果情報として、上記更新リクエストを受諾する旨を示す受諾情報を上記電子機器に対して送信することを特徴とする請求項２５記載の複製機器検出システム。
【請求項３２】　正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、
所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを上記認証装置によって検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証工程と、
上記更新間隔検証工程による検証の結果に応じた検証結果情報を上記認証装置から上記電子機器に対して送信する送信工程とを備えることを特徴とする複製機器検出方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する電子機器及び認証装置、並びに複製機器検出システム及び複製機器検出方法に関する。
【０００２】
【従来の技術】近年、ネットワーク技術の進歩に伴い、いわゆるインターネット等を利用した電子商取引やオンラインショッピング等の各種サービスが普及しつつある。また、ネットワークに接続可能な機器としては、パーソナルコンピュータのような情報処理装置のみならず、例えばディジタルテレビやディジタル衛星放送向けのセットトップボックス等の各種ＡＶ（Audio/Visual）機器も、ネットワークを介して相互に接続することが可能となりつつある。
【０００３】このようなネットワークシステムにおいては、機器間の通信を行うにあたって、データの盗聴や改竄等の行為による危険を防止するために、通信相手の正当性を認証するための相互認証を行う必要がある。このような機器間認証としては、通常、機器が正当であるか否かを検証するものではなく、当該機器自体は正当であることを前提とした上で、当該機器が所定のサービスを受ける権利を有するものであるか否かを検証するものが多い。
【０００４】具体的には、機器間認証としては、いわゆる共通鍵暗号方式に基づいたチャレンジ／レスポンス型認証が多く用いられる。このチャレンジ／レスポンス型認証とは、認証を受ける機器が固有の秘密情報を有していることを確認することにより、当該機器を認証する方式であり、機器を操作するユーザが所定のチャレンジコードに対するレスポンスコードを入力することにより、正当な機器であることを認証するものである。
【０００５】すなわち、共通鍵暗号方式に基づいた認証を行うネットワークシステムにおいては、機器の認証を行う際には、まず、認証を行う所定の認証装置が、機器に対して所定のチャレンジコードに対するレスポンスコードを返すようにリクエストを行う。そして、ネットワークシステムにおいては、このリクエストに応じて機器が認証装置に対してレスポンスを行うと、認証装置がレスポンスの内容を検証し、当該機器の正当性を判別す

る。

【０００６】このように、ネットワークシステムにおいては、共通鍵暗号方式に基づいたチャレンジ／レスポンス型認証を用いることにより、機器間認証を行うことができる。

【０００７】

【発明が解決しようとする課題】ところで、上述した共通鍵暗号方式に基づいた認証を行うネットワークシステムにおいては、正当な機器が固有に有する各種情報の一部を複製することによって作製された電子機器である不完全な複製機器が接続された場合には、通常の機器間認証を行うことによって不当なものであることを検証することが可能である。しかしながら、ネットワークシステムにおいては、正当な機器が固有に有する各種情報の全てを複製することによって作製された電子機器である完全な複製機器が接続された場合には、正当な機器であるものと誤って認証されてしまうといった問題があった。

【０００８】本発明は、このような実情に鑑みてなされたものであり、不完全な複製機器のみならず、完全な複製機器であっても追跡（Traitor Tracing）し、複製機器の存在を検出することができる電子機器及び認証装置、並びに複製機器検出システム及び複製機器検出方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】上述した目的を達成する本発明にかかる電子機器は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する電子機器であって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、最後に公開鍵データを更新した時刻を示す更新時刻情報を認証装置から取得する取得手段と、現在時刻を示す現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えることを特徴としている。

【００１０】このような本発明にかかる電子機器は、現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、更新間隔検証手段によって公開鍵データの更新間隔の整合性を検証する。

【００１１】また、上述した目的を達成する本発明にかかる認証装置は、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置であって、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、この更新間隔検証手段による検証の結果に応じた検証結果情報を電子機器に対して送信する送信手段とを備えることを特徴としている。

【００１２】このような本発明にかかる認証装置は、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを更新間隔検証手段によって検証し、公開鍵データの更新間隔の整合性を検証する。

【００１３】さらに、上述した目的を達成する本発明にかかる複製機器検出システムは、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、電子機器は、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、最後に公開鍵データを更新した時刻を示す更新時刻情報を認証装置から取得する取得手段と、現在時刻を示す現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えることを特徴としている。

【００１４】このような本発明にかかる複製機器検出システムは、現在時刻情報と、電子機器によって取得した更新時刻情報と、電子機器によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証する。

【００１５】さらにまた、上述した目的を達成する本発明にかかる複製機器検出方法は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する電子機器による公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を電子機器によって発生する乱数発生工程と、最後に公開鍵データを更新した時刻を示す更新時刻情報を電子機器によって認証装置から取得する取得工程と、現在時刻を示す現在時刻情報と、取得工程にて取得した更新時刻情報と、乱数発生工程にて前回の公開鍵データの更新時に発

生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証する更新間隔検証工程とを備えることを特徴としている。

【００１６】このような本発明にかかる複製機器検出方法は、現在時刻情報と、電子機器によって取得した更新時刻情報と、電子機器によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証する。

【００１７】また、上述した目的を達成する本発明にかかる複製機器検出システムは、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置は、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、この更新間隔検証手段による検証の結果に応じた検証結果情報を電子機器に対して送信する送信手段とを備えることを特徴としている。

【００１８】このような本発明にかかる複製機器検出システムは、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証する。

【００１９】さらに、上述した目的を達成する本発明にかかる複製機器検出方法は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証工程と、この更新間隔検証工程による検証の結果に応じた検証結果情報を認証装置から電子機器に対して送信する送信工程とを備えることを特徴としている。

【００２０】このような本発明にかかる複製機器検出方法は、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証する。

【００２１】

【発明の実施の形態】以下、本発明を適用した具体的な実施の形態について図面を参照しながら詳細に説明する。

【００２２】この実施の形態は、例えば図１に示すように、ＬＡＮ（Local Area Network）等の所定のネットワークを介して相互に接続された複数の電子機器１０，２０の間でデータの送受信を行うことができるデータ送受信システムである。特に、このデータ送受信システムは、正当な電子機器が固有に有する各種情報の一部を複製することによって作製された電子機器である不完全な複製機器が接続された場合のみならず、正当な機器が固有に有する各種情報の全てを複製することによって作製された電子機器である完全な複製機器が接続された場合であっても、複製機器を追跡（Traitor Tracing）し、複製機器の存在を検出することができるものである。

【００２３】このデータ送受信システムは、従来の共通鍵暗号方式に基づく機器間認証（authentication）を行うものではなく、鍵の配送に関する安全面が向上するとともに鍵の管理が容易であるいわゆる公開鍵暗号方式に基づく機器間認証を行うものである。そこで、ここでは、複製機器の追跡機能についての説明に先だって、公開鍵暗号方式に基づく公開鍵データの登録（registration）、機器間認証、及び登録又は更新（renewal）された公開鍵データの更新について説明するものとする。

【００２４】データ送受信システムは、例えば図１に示すように、相互に接続された電子機器１０，２０と、これらの電子機器１０，２０の認証を行う公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関（Certification Authority）ＣＡが有する認証装置３０とがインターネットＮＥＴを介して接続されて構成される。なお、データ送受信システムにおいては、認証機関ＣＡは、１つではなく、電子機器１０，２０のそれぞれに対応して２つ設けてもよい。

【００２５】電子機器１０，２０は、それぞれ、例えば、パーソナルコンピュータのような情報処理装置の他、ディジタルテレビやディジタル衛星放送向けのセットトップボックス等の各種ＡＶ（Audio/Visual）機器として構成され、耐タンパー処理がなされて構成される。電子機器１０，２０は、それぞれ、図２に示すように、各部を統括的に制御するＣＰＵ（Central Processing Unit）１１と、このＣＰＵ１１のワークエリアとして機能するＲＡＭ（Random Access Memory）１２と、ＣＰＵ１１によって実行される各種プログラムを含む情報を格納する読み取り専用のＲＯＭ（Read Only Memory）１３

と、各種データを記憶する電気的に書き換え可能なＲＯＭであるＥＥＰＲＯＭ（Electrically Erasable Programmable Read-Only Memory）１４との他に、乱数データを発生する乱数発生部１５と、この乱数発生部１５によって発生した乱数データを用いて公開鍵暗号方式に用いられる所定の鍵データを生成する鍵生成部１６と、公開鍵暗号方式における暗号化及び復号を行う暗号化／復号部１７と、外部とデータの送受信を行う通信部１８とを備える。電子機器１０，２０は、それぞれ、これらのＣＰＵ１１、ＲＡＭ１２、ＲＯＭ１３、ＥＥＰＲＯＭ１４、乱数発生部１５、鍵生成部１６、暗号化／復号部１７、及び通信部１８がバス１９を介して接続されて構成される。

【００２６】なお、この電子機器１０，２０は、それぞれ、乱数発生部１５による乱数発生処理、並びに鍵生成部１６及び暗号化／復号部１７による公開鍵暗号方式に関連する機能を実現する暗号エンジンとしての処理を行うが、この機能をハードウェアで実現するのみならず、コンピュータ実行可能なソフトウェアで実現することもできる。電子機器１０，２０は、それぞれ、ソフトウェアで実現する場合には、ＣＰＵ１１によって乱数発生処理及び暗号エンジンとしての処理を提供するための所定のプログラムを実行することにより、この機能を実現することができる。このプログラムは、例えばいわゆるコンパクトディスク（Compact Disc；ＣＤ）等のコンピュータ実行可能な所定の記録媒体やインターネット等の伝送媒体によって提供することができる。

【００２７】ＣＰＵ１１は、更新間隔検証手段、更新時刻情報検証手段、及び検証結果情報検証手段として機能するものであり、バス１９を介して、ＲＡＭ１２、ＲＯＭ１３、ＥＥＰＲＯＭ１４、乱数発生部１５、鍵生成部１６、暗号化／復号部１７、及び通信部１８と接続し、各部を統括的に制御する。また、ＣＰＵ１１は、図示しないタイマーを有し、このタイマーによって後述するタイマー値を計数したり、現在時刻を提示する。

【００２８】ＲＡＭ１２は、ＣＰＵ１１が各種プログラムを実行する際のワークエリアとして機能し、ＣＰＵ１１の制御のもとに、各種データを一時記憶する。

【００２９】ＲＯＭ１３は、各種プログラムや、必要に応じて当該電子機器１０，２０がそれぞれ固有に有する情報である機器固有情報を含む各種データ等の各種情報を格納している。このＲＯＭ１３に格納されている各種プログラムは、ＣＰＵ１１の制御のもとに読み出されて実行されるとともに、このＲＯＭ１３に格納されている各種データは、ＣＰＵ１１の制御のもとに読み出される。

【００３０】記憶手段であるＥＥＰＲＯＭ１４は、電気的に消去、すなわち、書き換え可能なＲＯＭであり、ＣＰＵ１１の制御のもとに、上述した機器固有情報や認証機関ＣＡによって発行された公開鍵証明書を含む各種データを記憶する。また、このＥＥＰＲＯＭ１４に記憶されている各種データは、ＣＰＵ１１の制御のもとに読み出される。

【００３１】乱数発生部１５は、通信相手の正当性を認証するための相互認証や、この認証後に行うデータ通信の安全性を確保するための暗号化通信に使用する鍵生成の過程等において用いられる乱数データを発生する。この乱数発生部１５によって発生された乱数データは、鍵生成部１６によって用いられる。また、乱数発生部１５は、後述するように、乱数発生手段として、所定の乱数値を発生する。

【００３２】鍵生成部１６は、所定の公開鍵暗号方式における鍵生成アルゴリズムに基づいて、乱数発生部１５によって発生された乱数データを用いて、公開鍵暗号方式における秘密鍵データ及び公開鍵データを生成する。この鍵生成部１６によって生成された秘密鍵データ及び公開鍵データは、暗号化／復号部１７によって用いられる。

【００３３】暗号化／復号部１７は、鍵生成部１６によって生成された公開鍵データを用いて、所定の公開鍵暗号方式における暗号化を施す。また、暗号化／復号部１７は、復号手段として、鍵生成部１６によって生成された秘密鍵データを用いて、所定の公開鍵暗号方式における暗号化が施されたデータを復号する。

【００３４】通信部１８は、送信手段及び取得手段として機能するものであり、暗号化／復号部１７によって暗号化が施されたデータや所定の制御信号を外部へと送信するとともに、外部から暗号化が施されたデータを受信する。

【００３５】このような電子機器１０，２０は、それぞれ、後述する所定の通信プロトコルにしたがって、相互に機器間認証を行いつつ、データの送受信を行う。電子機器１０，２０は、それぞれ、外部へとデータを送信する場合には、鍵生成部１６によって生成した所定の公開鍵データを用いて、暗号化／復号部１７によって暗号化を施す。また、電子機器１０，２０は、外部からデータを受信した場合には、鍵生成部１６によって生成した所定の秘密鍵データを用いて、暗号化／復号部１７によって復号を施す。このとき、電子機器１０，２０は、それぞれ、公開鍵暗号アルゴリズムとしては任意のものを用いることができ、例えばＲＳＡ（Rivest-Shamir-Adleman）暗号方式や楕円曲線暗号方式（Elliptic Curve Cipher）等を用いることができる。

【００３６】なお、電子機器１０，２０は、それぞれ、鍵生成部１６及び暗号化／復号部１７を公開鍵暗号方式に関連する機能を実現する暗号エンジンとして用いるのみならず、これらの処理に加え、共通鍵暗号方式に関連する機能、特に鍵生成機能を実現する暗号エンジンを併有してもよく、さらに、いわゆるＳＨＡ１（Secure Hash Algorithm 1）処理等のハッシュ関数を実現する機能

を併有してもよい。

【００３７】一方、認証装置３０は、認証機関ＣＡが有するものであって、電子機器１０，２０のそれぞれに対して所定の公開鍵証明書を発行し、電子機器１０，２０のそれぞれの認証を行う。また、認証装置３０は、各種情報を記憶する図示しないリポジトリを有し、機器固有情報や公開鍵データの他、後述するように、最後に鍵データを更新した時刻を示す時刻情報や、電子機器１０，２０によってアクセスされた時刻を示す時刻情報といった各種情報をリポジトリに記憶させる。

【００３８】このような電子機器１０，２０及び認証装置３０から構成されるデータ送受信システムにおいては、後述する所定の通信プロトコルにしたがって、電子機器１０，２０のそれぞれから認証機関ＣＡにおける認証装置３０に対して公開鍵データが登録される。そして、データ送受信システムにおいては、後述する所定の通信プロトコルにしたがって、電子機器１０，２０が相互に機器間認証を行いつつ、データの送受信が行われる。さらに、データ送受信システムにおいては、後述する所定の通信プロトコルにしたがって、電子機器１０，２０のそれぞれによって認証機関ＣＡに対して登録又は更新された公開鍵データの更新が行われる。データ送受信システムにおいては、後述するように、この認証機関ＣＡに対する公開鍵データの更新時に、複製機器の存在が検出される。

【００３９】さて、このようなデータ送受信システムにおいては、電子機器１０，２０のそれぞれがインターネットＮＥＴに接続されると、これらの電子機器１０，２０のそれぞれから認証機関ＣＡに対して公開鍵データが登録される。なお、ここでは、電子機器１０，２０は、それぞれ、認証機関ＣＡによって発行された公開鍵証明書をＥＥＰＲＯＭ１４等に記憶しているものとする。また、ここでは、説明の便宜上、電子機器１０が公開鍵データを認証機関ＣＡに対して登録するものとして説明する。

【００４０】すなわち、データ送受信システムにおいては、図３に電子機器１０と認証機関ＣＡにおける認証装置３０との間の通信プロトコルを示すように、電子機器１０から認証装置３０に対しての公開鍵データの登録リクエストの通知、このリクエストを受信した認証装置３０から電子機器１０に対してのリクエストに対するレスポンスの通知、このレスポンスを受信した電子機器１０から認証装置３０に対しての登録情報の送信、及び登録情報を受信した認証装置３０から電子機器１０に対しての公開鍵データの登録完了又は復号エラーの通知が行われることにより、電子機器１０から認証機関ＣＡに対して公開鍵データが登録される。

【００４１】具体的には、データ送受信システムにおいては、図４に示すように、電子機器１０によって公開鍵データの登録のリクエストを行う旨の所定の操作を行うと、ステップＳ１において、電子機器１０は、認証装置３０に対して、ＣＰＵ１１の制御のもとに、公開鍵データの登録のリクエストを行う旨の所定の制御信号を通信部１８を介して送信する。

【００４２】これに応じて、データ送受信システムにおいては、ステップＳ２において、認証装置３０は、リクエストを受信する。そして、データ送受信システムにおいては、このリクエストを受信した認証装置３０によってリクエストに対するレスポンスを行う旨の所定の操作を行うと、ステップＳ３において、認証装置３０は、電子機器１０に対して、レスポンスとして、リクエストを受諾する旨の所定の制御信号を送信する。

【００４３】続いて、データ送受信システムにおいては、ステップＳ４において、電子機器１０は、通信部１８を介してレスポンスを受信すると、ステップＳ５において、ＣＰＵ１１の制御のもとに、認証機関ＣＡによって発行されてＥＥＰＲＯＭ１４等に記憶している公開鍵証明書Ｃｅｒｔ（ＣＡ）から、認証機関ＣＡの公開鍵データPK_{CA}を取り出す。そして、データ送受信システムにおいては、ステップＳ６において、電子機器１０は、この公開鍵データPK_{CA}を用いて、暗号化／復号部１７によって上述した機器固有情報ID_Mを暗号化し、暗号化機器固有情報Ｅ（PK_{CA}，ID_M）を生成する。データ送受信システムにおいては、ステップＳ７において、電子機器１０は、生成した暗号化機器固有情報Ｅ（PK_{CA}，ID_M）と、鍵生成部１６によって生成した自己の公開鍵データPK_Mとを、登録情報として、通信部１８を介して認証装置３０に対して送信する。

【００４４】そして、データ送受信システムにおいては、ステップＳ８において、認証装置３０は、登録情報としての暗号化機器固有情報Ｅ（PK_{CA}，ID_M）及び公開鍵データPK_Mを受信すると、ステップＳ９において、認証機関ＣＡの秘密鍵データSK_{CA}を用いて暗号化機器固有情報Ｅ（PK_{CA}，ID_M）の復号を試みる。

【００４５】データ送受信システムにおいては、認証装置３０によって正常に復号を行うことができた場合には、認証装置３０は、電子機器１０が正当なものであると判断し、ステップＳ１０において、機器固有情報ID_Mに対する公開鍵データとして公開鍵データPK_Mをリポジトリ（repository）に記憶させて登録するとともに、公開鍵データPK_Mの登録処理が正常に完了した旨を通知するために、ステップＳ１１において、正常に登録処理が完了した旨の制御信号を電子機器１０に対して送信し、ステップＳ１２において、正常終了する。これに応じて、データ送受信システムにおいては、ステップＳ１３において、正常に登録処理が完了した旨の制御信号を電子機器１０が通信部１８を介して受信すると、ステップＳ１４において、電子機器１０は、正常終了す

る。

【００４６】一方、データ送受信システムにおいては、認証装置３０によって正常に復号を行うことができなかった場合には、ステップＳ１５において、認証装置３０は、警告として、復号エラーを示す制御信号を電子機器１０に対して送信し、ステップＳ１６において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ１７において、復号エラーを示す制御信号を電子機器１０が通信部１８を介して受信すると、ステップＳ１８において、電子機器１０は、エラー終了する。

【００４７】データ送受信システムにおいては、電子機器１０がインターネットＮＥＴに接続されると、このような一連の処理を経ることにより、電子機器１０から認証機関ＣＡに対して公開鍵データPK_Mを登録することができる。データ送受信システムにおいては、電子機器１０によって機器固有情報ID_Mを認証機関ＣＡの公開鍵データPK_{CA}を用いて暗号化することにより、高い安全性のもとに、公開鍵データPK_Mの登録を行うことができる。勿論、電子機器２０についても同様の処理を経ることにより、認証機関ＣＡに対して自己の公開鍵データを登録することができる。

【００４８】なお、データ送受信システムにおいては、電子機器１０が認証機関ＣＡによって発行された公開鍵証明書をＥＥＰＲＯＭ１４等に記憶していない場合には、電子機器１０は、公開鍵データPK_Mの登録リクエストを行う際に、認証装置３０に対して公開鍵証明書Ｃｅｒｔ（ＣＡ）をリクエストし、受信した公開鍵証明書Ｃｅｒｔ（ＣＡ）に対する認証機関ＣＡの電子署名を検証すればよい。また、データ送受信システムにおいては、暗号化機器固有情報Ｅ（PK_{CA}，ID_M）及び公開鍵データPK_Mを登録情報とするのではなく、電子機器１０は、公開鍵データPK_{CA}を用いて、機器固有情報ID_Mとともに自己の公開鍵データPK_Mをも暗号化し、登録情報としてもよい。さらに、データ送受信システムにおいては、電子機器１０は、登録情報である暗号化機器固有情報Ｅ（PK_{CA}，ID_M）及び公開鍵データPK_Mに対して自己の秘密鍵データSK_Mを用いて電子署名を生成し、添付するようにしてもよい。

【００４９】つぎに、データ送受信システムにおける機器間認証について説明する。データ送受信システムにおいては、上述した公開鍵データPK_Mの登録が行われると、電子機器１０，２０の間でのデータの送受信に先だって、機器間認証が行われる。なお、ここでは、電子機器１０，２０は、それぞれ、認証機関ＣＡによって発行された公開鍵証明書をＥＥＰＲＯＭ１４等に記憶しているものとする。また、ここでは、電子機器１０から電子機器２０に対して機器間認証のリクエストを行うものとする。さらに、ここでは、説明の便宜上、電子機器１０の認証機関を認証機関ＣＡ１０と称するとともに、この認証機関ＣＡ１０が有する認証装置を認証装置３０１０と称し、さらに、電子機器２０の認証機関を認証機関２０と称するとともに、この認証機関ＣＡ２０が有する認証装置を認証装置３０２０と称するものとして説明する。

【００５０】データ送受信システムにおいては、図５に電子機器１０，２０と認証装置３０１０，３０２０との間の通信プロトコルを示すように、４つのパートに大別された処理、すなわち、電子機器１０，２０の間での第１の処理、電子機器１０と認証装置３０２０との間での第２の処理、電子機器２０と認証装置３０１０との間での第３の処理、及び電子機器１０，２０の間での第４の処理を行う。

【００５１】すなわち、データ送受信システムにおいては、第１の処理として、電子機器１０から電子機器２０に対しての機器間認証のリクエストの通知、このリクエストを受信した電子機器２０から電子機器１０に対してのリクエストに対するレスポンスの通知、電子機器１０，２０の間での少なくとも公開鍵暗号アルゴリズム及びハッシュアルゴリズムからなる取り決め情報の相互送受信、及び電子機器１０，２０の間での認証情報の相互送受信が行われ、第２の処理として、電子機器１０から認証装置３０２０に対しての公開鍵証明書発行のリクエストの通知、このリクエストを受信した認証装置３０２０から電子機器１０に対してのリクエストに対するレスポンスの通知、このレスポンスを受信した電子機器１０から認証装置３０２０に対しての電子機器２０の暗号化機器固有情報の送信、及び暗号化機器固有情報を受信した認証装置３０２０から電子機器１０に対しての電子機器２０の公開鍵証明書の送信が行われ、第３の処理として、電子機器２０から認証装置３０１０に対しての公開鍵証明書発行のリクエストの通知、このリクエストを受信した認証装置３０１０から電子機器２０に対してのリクエストに対するレスポンスの通知、このレスポンスを受信した電子機器２０から認証装置３０１０に対しての電子機器１０の暗号化機器固有情報の送信、及び暗号化機器固有情報を受信した認証装置３０１０から電子機器２０に対しての電子機器１０の公開鍵証明書の送信が行われ、最後に第４の処理として、電子機器１０，２０の間での暗号化関数データ及び電子署名の相互送受信が行われることにより、電子機器１０，２０の間での機器間認証が行われる。

【００５２】具体的には、データ送受信システムにおいては、まず図６に示す一連の処理を経ることにより、第１の処理を行う。

【００５３】すなわち、データ送受信システムにおいては、同図に示すように、電子機器１０によって機器間認証のリクエストを行う旨の所定の操作を行うと、ステップＳ２１において、電子機器１０は、電子機器２０に対して、ＣＰＵ１１の制御のもとに、機器間認証のリクエ

ストを行う旨の所定の制御信号を通信部１８を介して送信する。

【００５４】これに応じて、データ送受信システムにおいては、ステップＳ２２において、電子機器２０は、通信部１８を介してリクエストを受信する。そして、データ送受信システムにおいては、このリクエストを受信した電子機器２０によってリクエストに対するレスポンスを行う旨の所定の操作を行うと、ステップＳ２３において、電子機器２０は、電子機器１０に対して、レスポンスとして、リクエストを受諾する旨の所定の制御信号を通信部１８を介して送信する。

【００５５】続いて、データ送受信システムにおいては、ステップＳ２４において、電子機器１０は、通信部１８を介してレスポンスを受信すると、ステップＳ２５及びステップＳ２６において、電子機器１０，２０は、それぞれ、ＣＰＵ１１の制御のもとに、機器間認証を行うために必要となる所定の取り決め情報を通信部１８を介して相互に送受信するとともに、この取り決め情報の内容の確認を示す所定の制御信号を通信部１８を介して相互に送受信する。ここでは、電子機器１０，２０は、それぞれ、取り決め情報として、自己が用いる公開鍵暗号アルゴリズムとハッシュアルゴリズムとの他、必要に応じて、所定の臨時データ（nonce data）を相互に送受信する。

【００５６】そして、データ送受信システムにおいては、ステップＳ２７において、電子機器１０は、自己の認証機関ＣＡ１０によって発行されてＥＥＰＲＯＭ１４等に記憶している公開鍵証明書Ｃｅｒｔ（ＣＡ１０）から、認証機関ＣＡ１０の公開鍵データＰＫＣＡ１０を取り出す。そして、データ送受信システムにおいては、ステップＳ２８において、電子機器１０は、この公開鍵データＰＫＣＡ１０を用いて、暗号化／復号部１７によって上述した機器固有情報ＩＤＭ１０を暗号化し、暗号化機器固有情報Ｅ（ＰＫＣＡ１０，ＩＤＭ１０）を生成する。データ送受信システムにおいては、ステップＳ２９において、電子機器１０は、生成した暗号化機器固有情報Ｅ（ＰＫＣＡ１０，ＩＤＭ１０）と、公開鍵証明書Ｃｅｒｔ（ＣＡ１０）とを、認証情報として、通信部１８を介して電子機器２０に対して送信する。

【００５７】一方、データ送受信システムにおいては、ステップＳ３０において、電子機器２０は、自己の認証機関ＣＡ２０によって発行されてＥＥＰＲＯＭ１４等に記憶している公開鍵証明書Ｃｅｒｔ（ＣＡ２０）から、認証機関ＣＡ２０の公開鍵データＰＫＣＡ２０を取り出す。そして、データ送受信システムにおいては、ステップＳ３１において、電子機器２０は、この公開鍵データＰＫＣＡ２０を用いて、暗号化／復号部１７によって上述した機器固有情報ＩＤＭ２０を暗号化し、暗号化機器固有情報Ｅ（ＰＫＣＡ２０，ＩＤＭ２０）を生成する。データ送受信システムにおいては、ステップＳ３２において、電子機器２０は、生成した暗号化機器固有情報Ｅ（ＰＫＣＡ２０，ＩＤＭ２０）と、公開鍵証明書Ｃｅｒｔ（ＣＡ２０）とを、認証情報として、通信部１８を介して電子機器１０に対して送信する。

【００５８】続いて、データ送受信システムにおいては、ステップＳ２９において、電子機器２０から認証情報としての暗号化機器固有情報Ｅ（ＰＫＣＡ２０，ＩＤＭ２０）及び公開鍵証明書Ｃｅｒｔ（ＣＡ２０）を受信した電子機器１０は、ステップＳ３３において、ＣＰＵ１１の制御のもとに、公開鍵証明書Ｃｅｒｔ（ＣＡ２０）に対する電子署名の検証を行うことによって公開鍵証明書Ｃｅｒｔ（ＣＡ２０）の検証を行う。

【００５９】データ送受信システムにおいては、電子機器１０による公開鍵証明書Ｃｅｒｔ（ＣＡ２０）の検証の結果、公開鍵証明書Ｃｅｒｔ（ＣＡ２０）が正当なものであると判定された場合には、第２の処理及び第３の処理へと移行する。一方、データ送受信システムにおいては、電子機器１０による公開鍵証明書Ｃｅｒｔ（ＣＡ２０）の検証の結果、公開鍵証明書Ｃｅｒｔ（ＣＡ２０）が不当なものであると判定された場合には、ステップＳ３４において、電子機器１０は、警告として、公開鍵証明書エラーを示す制御信号を通信部１８を介して電子機器２０に対して送信し、ステップＳ３５において、エラー終了する。これに応じて、データ送受信システムにおいては、公開鍵証明書エラーを示す制御信号を電子機器２０が通信部１８を介して受信すると、ステップＳ３８において、電子機器２０は、エラー終了する。

【００６０】一方、データ送受信システムにおいては、ステップＳ３２において、電子機器１０から認証情報としての暗号化機器固有情報Ｅ（ＰＫＣＡ１０，ＩＤＭ１０）及び公開鍵証明書Ｃｅｒｔ（ＣＡ１０）を受信した電子機器２０は、ステップＳ３６において、ＣＰＵ１１の制御のもとに、公開鍵証明書Ｃｅｒｔ（ＣＡ１０）に対する電子署名の検証を行うことによって公開鍵証明書Ｃｅｒｔ（ＣＡ１０）の検証を行う。

【００６１】データ送受信システムにおいては、電子機器２０による公開鍵証明書Ｃｅｒｔ（ＣＡ１０）の検証の結果、公開鍵証明書Ｃｅｒｔ（ＣＡ１０）が正当なものであると判定された場合には、第２の処理及び第３の処理へと移行する。一方、データ送受信システムにおいては、電子機器２０による公開鍵証明書Ｃｅｒｔ（ＣＡ１０）の検証の結果、公開鍵証明書Ｃｅｒｔ（ＣＡ１０）が不当なものであると判定された場合には、ステップＳ３７において、電子機器２０は、警告として、公開鍵証明書エラーを示す制御信号を通信部１８を介して電子機器１０に対して送信し、ステップＳ３８において、エラー終了する。これに応じて、データ送受信システムにおいては、公開鍵証明書エラーを示す制御信号を電子機器１０が通信部１８を介して受信すると、ステップＳ３５において、電子機器１０は、エラー終了する。

【００６２】データ送受信システムにおいては、このような第１の処理を経て、公開鍵証明書Ｃｅｒｔ（ＣＡ１０），Ｃｅｒｔ（ＣＡ２０）が正当なものであると判定された場合には、第２の処理及び第３の処理へと移行する。

【００６３】まず、第２の処理について説明する。データ送受信システムにおいては、図７に示す一連の処理を経ることにより、第２の処理を行う。

【００６４】すなわち、データ送受信システムにおいては、同図に示すように、電子機器１０によって電子機器２０の公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）の発行のリクエストを行う旨の所定の操作を行うと、ステップＳ４１において、電子機器１０は、認証装置３０２０に対して、ＣＰＵ１１の制御のもとに、公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）の発行のリクエストを行う旨の所定の制御信号を通信部１８を介して送信する。

【００６５】これに応じて、データ送受信システムにおいては、ステップＳ４２において、認証装置３０２０は、リクエストを受信する。そして、データ送受信システムにおいては、このリクエストを受信した認証装置３０２０によってリクエストに対するレスポンスを行う旨の所定の操作を行うと、ステップＳ４３において、認証装置３０２０は、電子機器１０に対して、レスポンスとして、リクエストを受諾する旨の所定の制御信号を送信する。

【００６６】続いて、データ送受信システムにおいては、ステップＳ４４において、電子機器１０は、通信部１８を介してレスポンスを受信すると、ステップＳ４５において、上述した第１の処理にて電子機器２０から送信されてきた暗号化機器固有情報Ｅ（ＰＫＣＡ２０，ＩＤＭ２０）を通信部１８を介して認証装置３０２０に対して送信する。

【００６７】そして、データ送受信システムにおいては、ステップＳ４６において、認証装置３０２０は、暗号化機器固有情報Ｅ（ＰＫＣＡ２０，ＩＤＭ２０）を受信すると、ステップＳ４７において、認証機関ＣＡ２０の秘密鍵データＳＫＣＡ２０を用いて暗号化機器固有情報Ｅ（ＰＫＣＡ２０，ＩＤＭ２０）の復号を試みる。

【００６８】データ送受信システムにおいては、認証装置３０２０によって正常に復号を行うことができなかった場合には、ステップＳ５０において、認証装置３０２０は、警告として、認証情報エラーを示す制御信号を電子機器１０に対して送信し、ステップＳ５１において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ５２において、認証情報エラーを示す制御信号を電子機器１０が通信部１８を介して受信すると、ステップＳ５３において、電子機器１０は、エラー終了する。

【００６９】一方、データ送受信システムにおいては、認証装置３０２０によって正常に復号を行うことができた場合には、認証装置３０２０は、ステップＳ４８において、リポジトリを参照し、ステップＳ４９において、電子機器２０の機器固有情報ＩＤＭ２０がリポジトリに登録されているか否かを照合する。

【００７０】ここで、データ送受信システムにおいては、認証装置３０２０による照合の結果、機器固有情報ＩＤＭ２０がリポジトリに登録されていないものと判定された場合には、ステップＳ５０において、認証装置３０２０は、警告として、機器固有情報照合エラーを示す制御信号を電子機器１０に対して送信し、ステップＳ５１において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ５２において、機器固有情報照合エラーを示す制御信号を電子機器１０が通信部１８を介して受信すると、ステップＳ５３において、電子機器１０は、エラー終了する。

【００７１】一方、データ送受信システムにおいては、認証装置３０２０による照合の結果、機器固有情報ＩＤＭ２０がリポジトリに登録されているものと判定された場合には、認証装置３０２０は、ステップＳ５４において、リポジトリから機器固有情報ＩＤＭ２０を読み出し、ステップＳ５５において、電子機器２０の公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）を署名して発行し、ステップＳ５６において、この公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）を電子機器１０に対して送信する。

【００７２】データ送受信システムにおいては、ステップＳ５７において、公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）を電子機器１０が通信部１８を介して受信すると、ステップＳ５８において、電子機器１０は、ＣＰＵ１１の制御のもとに、公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）に対する認証装置３０２０の電子署名の検証を行うことによって公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）の検証を行う。

【００７３】データ送受信システムにおいては、電子機器１０による公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）の検証の結果、公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）が正当なものであると判定された場合には、第４の処理へと移行する。一方、データ送受信システムにおいては、電子機器１０による公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）の検証の結果、公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）が不当なものであると判定された場合には、ステップＳ５９において、電子機器１０は、警告として、公開鍵証明書エラーを示す制御信号を通信部１８を介して認証装置３０２０に対して送信し、ステップＳ６０において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ６１において、公開鍵証明書エラーを示す制御信号を認証装置３０２０が受信すると、ステップＳ６２において、認証装置３０２０は、エラー終了する。

【００７４】つぎに、第３の処理について説明する。データ送受信システムにおいては、図８に示す一連の処理

を経ることにより、第３の処理を行う。

【００７５】すなわち、データ送受信システムにおいては、同図に示すように、電子機器２０によって電子機器１０の公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）の発行のリクエストを行う旨の所定の操作を行うと、ステップＳ７１において、電子機器２０は、認証装置３０１０に対して、ＣＰＵ１１の制御のもとに、公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）の発行のリクエストを行う旨の所定の制御信号を通信部１８を介して送信する。

【００７６】これに応じて、データ送受信システムにおいては、ステップＳ７２において、認証装置３０１０は、リクエストを受信する。そして、データ送受信システムにおいては、このリクエストを受信した認証装置３０１０によってリクエストに対するレスポンスを行う旨の所定の操作を行うと、ステップＳ７３において、認証装置３０１０は、電子機器２０に対して、レスポンスとして、リクエストを受諾する旨の所定の制御信号を送信する。

【００７７】続いて、データ送受信システムにおいては、ステップＳ７４において、電子機器２０は、通信部１８を介してレスポンスを受信すると、ステップＳ７５において、上述した第１の処理にて電子機器１０から送信されてきた暗号化機器固有情報Ｅ（ＰＫＣＡ１０，ＩＤＭ１０）を通信部１８を介して認証装置３０１０に対して送信する。

【００７８】そして、データ送受信システムにおいては、ステップＳ７６において、認証装置３０１０は、暗号化機器固有情報Ｅ（ＰＫＣＡ１０，ＩＤＭ１０）を受信すると、ステップＳ７７において、認証機関ＣＡ１０の秘密鍵データＳＫＣＡ１０を用いて暗号化機器固有情報Ｅ（ＰＫＣＡ１０，ＩＤＭ１０）の復号を試みる。

【００７９】データ送受信システムにおいては、認証装置３０１０によって正常に復号を行うことができなかった場合には、ステップＳ８０において、認証装置３０１０は、警告として、認証情報エラーを示す制御信号を電子機器２０に対して送信し、ステップＳ８１において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ８２において、認証情報エラーを示す制御信号を電子機器２０が通信部１８を介して受信すると、ステップＳ８３において、電子機器２０は、エラー終了する。

【００８０】一方、データ送受信システムにおいては、認証装置３０１０によって正常に復号を行うことができた場合には、認証装置３０１０は、ステップＳ７８において、リポジトリを参照し、ステップＳ７９において、電子機器１０の機器固有情報ＩＤＭ１０がリポジトリに登録されているか否かを照合する。

【００８１】ここで、データ送受信システムにおいては、認証装置３０１０による照合の結果、機器固有情報ＩＤＭ１０がリポジトリに登録されていないものと判定された場合には、ステップＳ８０において、認証装置３０１０は、警告として、機器固有情報照合エラーを示す制御信号を電子機器２０に対して送信し、ステップＳ８１において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ８２において、機器固有情報照合エラーを示す制御信号を電子機器２０が通信部１８を介して受信すると、ステップＳ８３において、電子機器２０は、エラー終了する。

【００８２】一方、データ送受信システムにおいては、認証装置３０１０による照合の結果、機器固有情報ＩＤＭ１０がリポジトリに登録されているものと判定された場合には、認証装置３０１０は、ステップＳ８４において、リポジトリから機器固有情報ＩＤＭ１０を読み出し、ステップＳ８５において、電子機器１０の公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）を署名して発行し、ステップＳ８６において、この公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）を電子機器２０に対して送信する。

【００８３】データ送受信システムにおいては、ステップＳ８７において、公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）を電子機器２０が通信部１８を介して受信すると、ステップＳ８８において、電子機器２０は、ＣＰＵ１１の制御のもとに、公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）に対する認証装置３０１０の電子署名の検証を行うことによって公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）の検証を行う。

【００８４】データ送受信システムにおいては、電子機器２０による公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）の検証の結果、公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）が正当なものであると判定された場合には、第４の処理へと移行する。一方、データ送受信システムにおいては、電子機器２０による公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）の検証の結果、公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）が不当なものであると判定された場合には、ステップＳ８９において、電子機器２０は、警告として、公開鍵証明書エラーを示す制御信号を通信部１８を介して認証装置３０１０に対して送信し、ステップＳ９０において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ９１において、公開鍵証明書エラーを示す制御信号を認証装置３０１０が受信すると、ステップＳ９２において、認証装置３０１０は、エラー終了する。

【００８５】データ送受信システムにおいては、このような第２の処理及び第３の処理を経て、公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０），Ｃｅｒｔ（ＩＤＭ２０）が正当なものであると判定された場合には、第４の処理へと移行する。

【００８６】データ送受信システムにおいては、図９に示す一連の処理を経ることにより、第４の処理を行う。

【００８７】すなわち、データ送受信システムにおいては、同図に示すように、ステップＳ１０１において、電

子機器１０は、乱数発生部１５によって所定のランダム関数に基づいて乱数データｒＭ１０を発生する。

【００８８】続いて、データ送受信システムにおいては、電子機器１０は、ＥＥＰＲＯＭ１４等に記憶している自己の機器固有情報ＩＤＭ１０を取り出し、ステップＳ１０２において、ＣＰＵ１１の制御のもとに、乱数データｒＭ１０と機器固有情報ＩＤＭ１０とに対して所定の関数ｆを適用し、関数データｆ（ＩＤＭ１０，ｒＭ１０）を算出する。

【００８９】続いて、データ送受信システムにおいては、電子機器１０は、ステップＳ１０３において、ＣＰＵ１１の制御のもとに、上述した第２の処理にて取得した電子機器２０の公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）から、電子機器２０の公開鍵データＰＫＭ２０を取り出す。そして、データ送受信システムにおいては、ステップＳ１０４において、電子機器１０は、この公開鍵データＰＫＭ２０を用いて、暗号化／復号部１７によって関数データｆ（ＩＤＭ１０，ｒＭ１０）を暗号化し、暗号化関数データＥ（ＰＫＭ２０，ｆ（ＩＤＭ１０，ｒＭ１０））を生成し、さらに、ステップＳ１０５において、鍵生成部１６によって生成した自己の秘密鍵データＳＫＭ１０を用いて、暗号化関数データＥ（ＰＫＭ２０，ｆ（ＩＤＭ１０，ｒＭ１０））の電子署名ＳｉｇＭ１０を生成する。データ送受信システムにおいては、ステップＳ１０６において、電子機器１０は、生成した暗号化関数データＥ（ＰＫＭ２０，ｆ（ＩＤＭ１０，ｒＭ１０））と、この暗号化関数データＥ（ＰＫＭ２０，ｆ（ＩＤＭ１０，ｒＭ１０））に対する電子署名ＳｉｇＭ１０とを、通信部１８を介して電子機器２０に対して送信する。

【００９０】一方、データ送受信システムにおいては、ステップＳ１０７において、電子機器２０は、乱数発生部１５によって所定のランダム関数に基づいて乱数データｒＭ２０を発生する。

【００９１】続いて、データ送受信システムにおいては、電子機器２０は、ＥＥＰＲＯＭ１４等に記憶している自己の機器固有情報ＩＤＭ２０を取り出し、ステップＳ１０８において、ＣＰＵ１１の制御のもとに、乱数データｒＭ２０と機器固有情報ＩＤＭ２０とに対して所定の関数ｇを適用し、関数データｇ（ＩＤＭ２０，ｒＭ２０）を算出する。

【００９２】続いて、データ送受信システムにおいては、電子機器２０は、ステップＳ１０９において、ＣＰＵ１１の制御のもとに、上述した第３の処理にて取得した電子機器１０の公開鍵証明書Ｃｅｒｔ（ＩＤＭ１０）から、電子機器１０の公開鍵データＰＫＭ１０を取り出す。そして、データ送受信システムにおいては、ステップＳ１１０において、電子機器２０は、この公開鍵データＰＫＭ１０を用いて、暗号化／復号部１７によって関数データｇ（ＩＤＭ２０，ｒＭ２０）を暗号化し、暗号化関数データＥ（ＰＫＭ１０，ｇ（ＩＤＭ２０，ｒＭ２０））を生成し、さらに、ステップＳ１１１において、鍵生成部１６によって生成した自己の秘密鍵データＳＫＭ２０を用いて、暗号化関数データＥ（ＰＫＭ１０，ｇ（ＩＤＭ２０，ｒＭ２０））の電子署名ＳｉｇＭ２０を生成する。データ送受信システムにおいては、ステップＳ１１２において、電子機器２０は、生成した暗号化関数データＥ（ＰＫＭ１０，ｇ（ＩＤＭ２０，ｒＭ２０））と、この暗号化関数データＥ（ＰＫＭ１０，ｇ（ＩＤＭ２０，ｒＭ２０））に対する電子署名ＳｉｇＭ２０とを、通信部１８を介して電子機器１０に対して送信する。

【００９３】続いて、データ送受信システムにおいては、ステップＳ１０６において、電子機器２０から暗号化関数データＥ（ＰＫＭ１０，ｇ（ＩＤＭ２０，ｒＭ２０））及び電子署名ＳｉｇＭ２０を受信した電子機器１０は、ステップＳ１１３において、ＣＰＵ１１の制御のもとに、電子機器２０の公開鍵証明書Ｃｅｒｔ（ＩＤＭ２０）から、電子機器２０の公開鍵データＰＫＭ２０を取り出し、ステップＳ１１４において、暗号化関数データＥ（ＰＫＭ１０，ｇ（ＩＤＭ２０，ｒＭ２０））に対する電子署名ＳｉｇＭ２０の検証を行う。

【００９４】データ送受信システムにおいては、電子機器１０による電子署名ＳｉｇＭ２０の検証の結果、電子署名ＳｉｇＭ２０が不当なものであると判定された場合には、ステップＳ１１５において、電子機器１０は、警告として、電子署名エラーを示す制御信号を通信部１８を介して電子機器２０に対して送信し、ステップＳ１１６において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ１２１において、電子署名エラーを示す制御信号を電子機器２０が通信部１８を介して受信すると、ステップＳ１２２において、電子機器２０は、エラー終了する。一方、データ送受信システムにおいては、電子署名ＳｉｇＭ２０の検証の結果、電子署名ＳｉｇＭ２０が正当なものであると判定された場合には、ステップＳ１１７において、電子機器１０は、鍵生成部１６によって生成した自己の秘密鍵データＳＫＭ１０を用いて、電子機器２０から送信されてきた暗号化関数データＥ（ＰＫＭ１０，ｇ（ＩＤＭ２０，ｒＭ２０））の復号を試みる。

【００９５】データ送受信システムにおいては、電子機器１０によって正常に復号を行うことができなかった場合には、ステップＳ１１５において、電子機器１０は、警告として、復号エラーを示す制御信号を通信部１８を介して電子機器２０に対して送信し、ステップＳ１１６において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ１２１において、復号エラーを示す制御信号を電子機器２０が通信部１８を介して受信すると、ステップＳ１２２において、電子機

器２０は、エラー終了する。

【００９６】一方、データ送受信システムにおいては、電子機器１０によって正常に復号を行うことができた場合には、電子機器１０は、ステップＳ１１８において、関数データｆ（ＩＤM１０，ｒM１０）と、復号して得られた関数データｇ（ＩＤM２０，ｒM２０）とに対して所定のハッシュ関数Ｈａｓｈを適用し、Ｈａｓｈ（ｆ（ＩＤM１０，ｒM１０），ｇ（ＩＤM２０，ｒM２０））を共通鍵データ、すなわち、対称鍵（symmetric key）データとして生成して正常終了する。

【００９７】また、データ送受信システムにおいては、ステップＳ１１２において、電子機器１０から暗号化関数データＥ（ＰＫM２０，ｆ（ＩＤM１０，ｒM１０））及び電子署名ＳｉｇM１０を受信した電子機器２０は、ステップＳ１１９において、ＣＰＵ１１の制御のもとに、電子機器１０の公開鍵証明書Ｃｅｒｔ（ＩＤM１０）から、電子機器１０の公開鍵データＰＫM１０を取り出し、ステップＳ１２０において、暗号化関数データＥ（ＰＫM２０，ｆ（ＩＤM１０，ｒM１０））に対する電子署名ＳｉｇM１０の検証を行う。

【００９８】データ送受信システムにおいては、電子機器２０による電子署名ＳｉｇM１０の検証の結果、電子署名ＳｉｇM１０が不当なものであると判定された場合には、ステップＳ１２１において、電子機器２０は、警告として、電子署名エラーを示す制御信号を通信部１８を介して電子機器１０に対して送信し、ステップＳ１２２において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ１１５において、電子署名エラーを示す制御信号を電子機器１０が通信部１８を介して受信すると、ステップＳ１１６において、電子機器１０は、エラー終了する。一方、データ送受信システムにおいては、電子署名ＳｉｇM１０の検証の結果、電子署名ＳｉｇM１０が正当なものであると判定された場合には、ステップＳ１２３において、電子機器２０は、鍵生成部１６によって生成した自己の秘密鍵データＳＫM２０を用いて、電子機器１０から送信されてきた暗号化関数データＥ（ＰＫM２０，ｇ（ＩＤM１０，ｒM１０））の復号を試みる。

【００９９】データ送受信システムにおいては、電子機器２０によって正常に復号を行うことができなかった場合には、ステップＳ１２１において、電子機器２０は、警告として、復号エラーを示す制御信号を通信部１８を介して電子機器１０に対して送信し、ステップＳ１２２において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ１１５において、復号エラーを示す制御信号を電子機器１０が通信部１８を介して受信すると、ステップＳ１１６において、電子機器１０は、エラー終了する。

【０１００】一方、データ送受信システムにおいては、電子機器２０によって正常に復号を行うことができた場合には、電子機器２０は、ステップＳ１２４において、関数データｇ（ＩＤM２０，ｒM２０）と、復号して得られた関数データｆ（ＩＤM１０，ｒM１０）とに対して所定のハッシュ関数Ｈａｓｈを適用し、Ｈａｓｈ（ｆ（ＩＤM１０，ｒM１０），ｇ（ＩＤM２０，ｒM２０））を共通鍵データとして生成して正常終了する。

【０１０１】データ送受信システムにおいては、このような第１の処理乃至第４の処理からなる一連の処理を経ることにより、電子機器１０，２０の間での機器間認証を行うことができる。これにより、データ送受信システムにおいては、電子機器１０，２０が不当に機能追加や機能削除が施されて改造された不完全な複製機器ではなく、また、不当に偽造された不完全な複製機器ではないことが認証され、電子機器１０，２０の間でのデータの送受信が可能とされる。なお、上述した第２の処理及び第３の処理を正常終了した段階で、電子機器１０，２０は、それぞれ、互いの公開鍵証明書Ｃｅｒｔ（ＩＤM１０），Ｃｅｒｔ（ＩＤM２０）を取得していることから、データ送受信システムにおいては、第４の処理にて臨時データとして種々のパラメータを与えることにより、第４の処理として、無数のパターンを構築することができる。ここでは、データ送受信システムは、電子機器１０，２０が、それぞれ、互いの公開鍵証明書Ｃｅｒｔ（ＩＤM１０），Ｃｅｒｔ（ＩＤM２０）を取得することができること、及び共通鍵データを生成することができることにより、機器間認証を行うことができる。

【０１０２】なお、データ送受信システムにおいては、上述した乱数データｒM１０，ｒM２０を発生するのに用いるランダム関数としては、電子機器１０，２０の間で同一のものであってもよく、異なるものであってもよい。また、データ送受信システムにおいては、上述した関数ｆ及び関数ｇとしては、電子機器１０，２０の間で同一のものであってもよく、異なるものであってもよい。さらに、データ送受信システムにおいては、電子機器１０の認証機関ＣＡ１０と電子機器２０の認証機関ＣＡ２０とは、同一であってもよい。

【０１０３】また、データ送受信システムにおいては、電子機器１０，２０が、それぞれ、自己の認証機関ＣＡ１０，ＣＡ２０によって発行された公開鍵証明書をＥＥＰＲＯＭ１４等に記憶していない場合には、電子機器１０，２０は、それぞれ、自己の認証装置３０１０，３０２０に対して公開鍵証明書Ｃｅｒｔ（ＣＡ１０），Ｃｅｒｔ（ＣＡ２０）をリクエストし、受信した公開鍵証明書Ｃｅｒｔ（ＣＡ１０），Ｃｅｒｔ（ＣＡ２０）に対する認証機関ＣＡ１０，ＣＡ２０の電子署名を検証すればよい。また、データ送受信システムにおいては、電子機器１０，２０は、それぞれ、上述した認証情報の相互送受信の際や、認証装置３０１０，３０２０に対する暗号

化機器固有情報Ｅ（ＰＫＣＡ１０，ＩＤＭ１０），Ｅ（ＰＫＣＡ２０，ＩＤＭ２０）の送信の際に、自己が生成した電子署名を添付するようにしてもよい。

【０１０４】つぎに、データ送受信システムにおける登録又は更新された公開鍵データの更新について説明する。データ送受信システムにおいては、所定のタイミングで発せされる電子機器１０，２０のそれぞれからのリクエストに応じて、認証機関ＣＡに対して登録又は更新された公開鍵データが更新される。なお、ここでは、電子機器１０，２０は、それぞれ、認証機関ＣＡによって発行された公開鍵証明書をＥＥＰＲＯＭ１４等に記憶しているものとする。また、ここでは、説明の便宜上、電子機器１０が認証機関ＣＡに対して登録又は更新された公開鍵データを更新するものとして説明する。

【０１０５】すなわち、データ送受信システムにおいては、図１０に電子機器１０と認証機関ＣＡにおける認証装置３０との間の通信プロトコルを示すように、電子機器１０から認証装置３０に対しての公開鍵データの更新リクエストの通知、このリクエストを受信した認証装置３０から電子機器１０に対してのリクエストに対するレスポンスの通知、このレスポンスを受信した電子機器１０から認証装置３０に対しての更新情報の送信、及び更新情報を受信した認証装置３０から電子機器１０に対しての公開鍵データの更新完了又は復号エラー若しくは機器固有情報照合エラーの通知が行われることにより、電子機器１０から認証機関ＣＡに対して登録又は更新された公開鍵データが更新される。

【０１０６】具体的には、データ送受信システムにおいては、図１１に示すように、電子機器１０によって公開鍵データの更新のリクエストを行う旨の所定の操作を行うと、ステップＳ１３１において、電子機器１０は、認証装置３０に対して、ＣＰＵ１１の制御のもとに、公開鍵データの更新のリクエストを行う旨の所定の制御信号を通信部１８を介して送信する。

【０１０７】これに応じて、データ送受信システムにおいては、ステップＳ１３２において、認証装置３０は、リクエストを受信する。そして、データ送受信システムにおいては、このリクエストを受信した認証装置３０によってリクエストに対するレスポンスを行う旨の所定の操作を行うと、ステップＳ１３３において、認証装置３０は、電子機器１０に対して、レスポンスとして、リクエストを受諾する旨の所定の制御信号を送信する。

【０１０８】続いて、データ送受信システムにおいては、ステップＳ１３４において、電子機器１０は、通信部１８を介してレスポンスを受信すると、ステップＳ１３５において、ＣＰＵ１１の制御のもとに、認証機関ＣＡによって発行されてＥＥＰＲＯＭ１４等に記憶している公開鍵証明書Ｃｅｒｔ（ＣＡ）から、認証機関ＣＡの公開鍵データＰＫＣＡを取り出す。そして、データ送受信システムにおいては、ステップＳ１３６において、電子機器１０は、この公開鍵データＰＫＣＡを用いて、暗号化／復号部１７によって上述した機器固有情報ＩＤＭを暗号化し、暗号化機器固有情報Ｅ（ＰＫＣＡ，ＩＤＭ）を生成する。データ送受信システムにおいては、ステップＳ１３７において、電子機器１０は、生成した暗号化機器固有情報Ｅ（ＰＫＣＡ，ＩＤＭ）と、鍵生成部１６によって生成した自己の新たな公開鍵データＰＫＭｎｅｗとを、更新情報として、通信部１８を介して認証装置３０に対して送信する。

【０１０９】そして、データ送受信システムにおいては、ステップＳ１３８において、認証装置３０は、更新情報としての暗号化機器固有情報Ｅ（ＰＫＣＡ，ＩＤＭ）及び新たな公開鍵データＰＫＭｎｅｗを受信すると、ステップＳ１３９において、認証機関ＣＡの秘密鍵データＳＫＣＡを用いて暗号化機器固有情報Ｅ（ＰＫＣＡ，ＩＤＭ）の復号を試みる。

【０１１０】データ送受信システムにおいては、認証装置３０によって正常に復号を行うことができた場合には、認証装置３０は、ステップＳ１４０において、リポジトリを参照し、ステップＳ１４１において、復号して得られた機器固有情報ＩＤＭがリポジトリに登録されているか否かを照合する。

【０１１１】ここで、データ送受信システムにおいては、認証装置３０による照合の結果、機器固有情報ＩＤＭがリポジトリに登録されていないものと判定された場合には、ステップＳ１４８において、認証装置３０は、警告として、機器固有情報照合エラーを示す制御信号を電子機器１０に対して送信し、ステップＳ１４９において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ１５０において、機器固有情報照合エラーを示す制御信号を電子機器１０が通信部１８を介して受信すると、ステップＳ１５１において、電子機器１０は、エラー終了する。

【０１１２】一方、データ送受信システムにおいては、認証装置３０による照合の結果、機器固有情報ＩＤＭがリポジトリに登録されているものと判定された場合には、認証装置３０は、電子機器１０が前回公開鍵データの登録又は更新を行ったものと同一の正当なものであると判断し、ステップＳ１４２及びステップＳ１４３において、機器固有情報ＩＤＭに対する公開鍵データとして新たな公開鍵データＰＫＭｎｅｗをリポジトリに記憶させて更新するとともに、公開鍵データＰＫＭｎｅｗの更新処理が正常に完了した旨を通知するために、ステップＳ１４４において、正常に更新処理が完了した旨の制御信号を電子機器１０に対して送信し、ステップＳ１４５において、正常終了する。これに応じて、データ送受信システムにおいては、ステップＳ１４６において、正常に更新処理が完了した旨の制御信号を電子機器１０が通信部１８を介して受信すると、ステップＳ１４７において、電子機器１０は、正常終了する。

【０１１３】一方、データ送受信システムにおいては、認証装置３０によって正常に復号を行うことができなかった場合には、ステップＳ１４８において、認証装置３０は、警告として、復号エラーを示す制御信号を電子機器１０に対して送信し、ステップＳ１４９において、エラー終了する。これに応じて、データ送受信システムにおいては、ステップＳ１５０において、復号エラーを示す制御信号を電子機器１０が通信部１８を介して受信すると、ステップＳ１５１において、電子機器１０は、エラー終了する。

【０１１４】データ送受信システムにおいては、このような一連の処理を経ることにより、電子機器１０が認証機関ＣＡに対して登録又は更新された公開鍵データを新たな公開鍵データPK_{Mnew}に更新することができる。データ送受信システムにおいては、電子機器１０によって機器固有情報ID_Mを認証機関ＣＡの公開鍵データPK_{CA}を用いて暗号化することにより、高い安全性のもとに、公開鍵データPK_{Mnew}の更新を行うことができる。勿論、電子機器２０についても同様の処理を経ることにより、認証機関ＣＡに対して自己の公開鍵データを登録することができる。

【０１１５】なお、データ送受信システムにおいては、電子機器１０が認証機関ＣＡによって発行された公開鍵証明書をＥＥＰＲＯＭ１４等に記憶していない場合には、電子機器１０は、公開鍵データPK_{Mnew}の更新リクエストを行う際に、認証装置３０に対して公開鍵証明書Ｃｅｒｔ（ＣＡ）をリクエストし、受信した公開鍵証明書Ｃｅｒｔ（ＣＡ）に対する認証機関ＣＡの電子署名を検証すればよい。また、データ送受信システムにおいては、暗号化機器固有情報Ｅ（PK_{CA}，ID_M）及び公開鍵データPK_{Mnew}を更新情報とするのではなく、電子機器１０は、公開鍵データPK_{CA}を用いて、機器固有情報ID_Mとともに自己の公開鍵データPK_{Mnew}をも暗号化し、更新情報としてもよい。さらに、データ送受信システムにおいては、電子機器１０は、更新情報である暗号化機器固有情報Ｅ（PK_{CA}，ID_M）及び公開鍵データPK_{Mnew}に対して自己の古い秘密鍵データSK_M、又は自己の新たな秘密鍵データSK_{Mnew}を用いて電子署名を生成し、添付するようにしてもよい。

【０１１６】さて、データ送受信システムは、正当な電子機器が固有に有する各種情報の一部を複製することによって作製された電子機器である不完全な複製機器が接続された場合のみならず、正当な機器が固有に有する各種情報の全てを複製することによって作製された電子機器である完全な複製機器が接続された場合であっても、認証機関ＣＡに対する公開鍵データの更新時に、複製機器を追跡することができ、複製機器の存在を検出することができる。ここでは、説明の便宜上、正当な機器である電子機器１０とこの電子機器１０の複製機器とが接続された場合について説明する。

【０１１７】概念的には、データ送受信システムにおいては、公開鍵データの更新を行う際には、図１２に示すように、電子機器１０及び複製機器ともに、同様の動作を行う。すなわち、電子機器１０及び複製機器は、それぞれ、乱数値ｔを発生し、この発生した乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たすか否かを判定する。そして、電子機器１０及び複製機器は、それぞれ、乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たさない場合には、再度異なる乱数値ｔを発生し、この乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たすか否かを判定する。一方、電子機器１０及び複製機器は、それぞれ、乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たす場合には、新たな公開鍵データ及び秘密鍵データの対を生成し、先に図１０に示した更新処理のプロトコルにしたがって、先に図１１に示したような処理を行い、認証装置３０に対する公開鍵データの更新を行う。

【０１１８】ここで、データ送受信システムにおいては、機器固有情報ID_Mを有する機器の公開鍵データ及び秘密鍵データの対の更新間隔は、常に、予め規定された所定の範囲$T_1 \leqq t \leqq T_2$である必要があることに着目する。

【０１１９】すなわち、データ送受信システムにおいては、図１３（Ａ）に示すように、正当な機器である電子機器１０が常に所定の範囲$T_1 \leqq t \leqq T_2$の間隔で、更新のリクエストを認証装置３０に対して通知する場合であり、同図（Ｂ）に示すように、複製機器が電子機器１０の更新間隔と同間隔で、更新のリクエストを認証装置３０に対して通知する場合であっても、電子機器１０から認証装置３０に対してリクエストの通知が到達して受諾される時刻と、複製機器から認証装置３０に対してリクエストの通知が到達して受諾される時刻との間に差が生じることから、複製機器、特に完全な複製機器が存在する場合には、認証装置３０に対してリクエストの通知が到達する間隔は、同図（Ｃ）に示すように、例えば$t < T_1$といったように、所定の範囲$T_1 \leqq t \leqq T_2$から外れる。このとき、データ送受信システムにおいては、たとえ、電子機器１０から認証装置３０に対してリクエストの通知が発せられる時刻と、複製機器から認証装置３０に対してリクエストの通知が発せられる時刻とが同一であったとしても、認証装置３０によってリクエストを受諾する際には時間的なずれが生じることから、結果的に、認証装置３０に対してリクエストの通知が到達する間隔は、規定された所定の範囲$T_1 \leqq t \leqq T_2$から必然的に外れることとなる。

【０１２０】したがって、データ送受信システムにおいては、この鍵データの更新間隔のずれを検出することにより、複製機器を追跡し、複製機器の存在を検出することができる。

【０１２１】具体的には、データ送受信システムにおい

ては、図１４乃至図１６に示す一連の処理を経ることにより、複製機器を追跡し、その存在を検出する。

【０１２２】まず、鍵データの更新間隔の整合性の検証を電子機器１０によって行う場合について、図１４を用いて説明する。

【０１２３】データ送受信システムにおいては、同図に示すように、ステップＳ１６１において、電子機器１０は、ＣＰＵ１１の制御のもとに、上述したタイマーが計数するタイマー値が"０"であるか否かを判定する。データ送受信システムにおいては、タイマー値が"０"でないものと判定された場合には、ステップＳ１６２において、電子機器１０は、ＣＰＵ１１の制御のもとに、タイマー値を"１"だけデクリメントさせ、タイマー値が"０"であるか否かを再度判定する。

【０１２４】そして、データ送受信システムにおいては、電子機器１０は、このような処理をタイマー値が"０"となるまで繰り返し、タイマー値が"０"であるものと判定された場合には、ステップＳ１６３において、ＣＰＵ１１の制御のもとに、乱数発生部１５によって乱数値ｔを発生し、ステップＳ１６４において、ＣＰＵ１１の制御のもとに、この乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たすか否かを判定する。データ送受信システムにおいては、電子機器１０は、乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たさない場合には、ステップＳ１６３からの処理を繰り返し、発生した乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たすまで、乱数値ｔを発生する。

【０１２５】データ送受信システムにおいては、電子機器１０は、乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たす場合には、ステップＳ１６５において、ＣＰＵ１１の制御のもとに、この乱数値ｔを次回の鍵データの更新までの時間ｔｉｍｅｒ＿ｎとしてＥＥＰＲＯＭ１４等に記憶させる。

【０１２６】これと同時に、データ送受信システムにおいては、ステップＳ１６６において、電子機器１０は、認証装置３０に対して、ＣＰＵ１１の制御のもとに、最後に鍵データを更新した時刻を示す更新時刻情報Ｔｌａｓｔのリクエストを行う旨の所定の制御信号を通信部１８を介して送信する。なお、ここでの更新時刻情報Ｔｌａｓｔは、最後に先に図１１に示したステップＳ１４２及びステップＳ１４３にて新たな公開鍵データＰＫＭｎｅｗをリポジトリに記憶させて更新した時刻を示すものとする。いずれにせよ、認証装置３０は、この更新時刻情報Ｔｌａｓｔをリポジトリ等に記憶している必要がある。

【０１２７】これに応じて、データ送受信システムにおいては、ステップＳ１６７において、認証装置３０は、リクエストを受信すると、電子機器１０の公開鍵データPK_Mを用いてリクエストされた更新時刻情報Ｔｌａｓｔを暗号化し、暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）を生成するとともに、認証機関ＣＡの秘密鍵データSK_{CA}を用いて暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）の電子署名Ｓｉｇを生成し、ステップＳ１６８において、レスポンスとして、生成した暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）と、この暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）に対する電子署名Ｓｉｇとを、電子機器１０に対して送信する。

【０１２８】続いて、データ送受信システムにおいては、ステップＳ１６９において、電子機器１０は、認証装置３０から暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）及び電子署名Ｓｉｇを受信すると、ステップＳ１７０において、ＣＰＵ１１の制御のもとに、電子署名Ｓｉｇの検証を行うことによって暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）の検証を行う。

【０１２９】データ送受信システムにおいては、電子機器１０による暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）の検証の結果、暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）が不当なものであると判定された場合には、ステップＳ１７３において、電子機器１０は、警告として、暗号化更新時刻情報エラーを示す制御信号を通信部１８を介して認証装置３０に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化更新時刻情報エラーを示す制御信号を認証装置３０が受信すると、認証装置３０は、エラー終了する。

【０１３０】一方、データ送受信システムにおいては、電子機器１０による暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）の検証の結果、暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）が正当なものであると判定された場合には、ステップＳ１７１において、電子機器１０は、ＣＰＵ１１の制御のもとに、現在時刻を示す現在時刻情報Ｔｎｏｗと、暗号化／復号部１７によって暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）を復号して得られた更新時刻情報Ｔｌａｓｔと、前回のタイマー値、すなわち、前回の鍵データの更新時にステップＳ１６５においてＥＥＰＲＯＭ１４等に記憶させた時間ｔｉｍｅｒ＿ｎに相当するタイマー値ｔｉｍｅｒとに基づいて、

$$T_{now} - (T_{last} + timer) \leqq \varepsilon$$

を満たすか否かを判定する。ここで、定数εは、電子機器１０と認証装置３０との間でのパケットの受け渡しに要する時間や、電子機器１０の内部での処理時間等を吸収する固定値である。また、現在時刻情報Ｔｎｏｗは、このステップＳ１７１における時刻を示すものとする。

【０１３１】データ送受信システムにおいては、$T_{now} - (T_{last} + timer) \leqq \varepsilon$を満たすものと判定された場合には、複製機器が存在していないことを示すことから、ステップＳ１７２において、電子機器１０は、鍵データの更新処理へと移行し、先に図１０に示した更新処理のプロトコルにしたがって、先に図１１に示したような処理を行い、認証装置３０に対する公開鍵データの更新を行う。

【０１３２】一方、データ送受信システムにおいては、Ｔｎｏｗ－（Ｔｌａｓｔ＋ｔｉｍｅｒ）≦εを満たさないものと判定された場合には、複製機器が存在していることを示すことから、ステップＳ１７３において、電子機器１０は、警告を発し、認証装置３０に対してその旨を通知するとともに、複製機器に対抗するための所定の処理へと移行する。電子機器１０は、複製機器に対抗するための所定の処理として、例えば、自己が提供するサービスを停止する処理や、自己の電源を遮断する処理といった種々の処理を行うことができる。

【０１３３】このように、データ送受信システムは、鍵データの更新間隔の整合性の検証を電子機器１０の側で行うことにより、複製機器を追跡してその存在を検出することができる。

【０１３４】つぎに、鍵データの更新間隔の整合性の検証を認証装置３０によって行う場合について、図１５を用いて説明する。

【０１３５】データ送受信システムにおいては、同図に示すように、ステップＳ１８１において、電子機器１０は、ＣＰＵ１１の制御のもとに、上述したタイマーが計数するタイマー値が"０"であるか否かを判定する。データ送受信システムにおいては、タイマー値が"０"でないものと判定された場合には、ステップＳ１８２において、電子機器１０は、ＣＰＵ１１の制御のもとに、タイマー値を"１"だけデクリメントさせ、タイマー値が"０"であるか否かを再度判定する。

【０１３６】そして、データ送受信システムにおいては、電子機器１０は、このような処理をタイマー値が"０"となるまで繰り返し、タイマー値が"０"であるものと判定された場合には、ステップＳ１８３において、ＣＰＵ１１の制御のもとに、乱数発生部１５によって乱数値ｔを発生し、ステップＳ１８４において、ＣＰＵ１１の制御のもとに、この乱数値ｔが所定の範囲Ｔ１≦ｔ≦Ｔ２を満たすか否かを判定する。データ送受信システムにおいては、電子機器１０は、乱数値ｔが所定の範囲Ｔ１≦ｔ≦Ｔ２を満たさない場合には、ステップＳ１８３からの処理を繰り返し、発生した乱数値ｔが所定の範囲Ｔ１≦ｔ≦Ｔ２を満たすまで、乱数値ｔを発生する。

【０１３７】データ送受信システムにおいては、電子機器１０は、乱数値ｔが所定の範囲Ｔ１≦ｔ≦Ｔ２を満たす場合には、ステップＳ１８５において、ＣＰＵ１１の制御のもとに、この乱数値ｔを次回の鍵データの更新までの時間ｔｉｍｅｒ＿ｎとしてＥＥＰＲＯＭ１４等に記憶させる。

【０１３８】これと同時に、データ送受信システムにおいては、ステップＳ１８６において、電子機器１０は、認証装置３０に対して、ＣＰＵ１１の制御のもとに、鍵データの更新のリクエストを行う旨の所定の制御信号を通信部１８を介して送信する。

【０１３９】これに応じて、データ送受信システムにおいては、ステップＳ１８７において、認証装置３０は、リクエストを受信すると、ステップＳ１８８において、最後に鍵データを更新した時刻を示す更新時刻情報Ｔｌａｓｔと、電子機器１０によってアクセスされた時刻を示すアクセス時刻情報Ｔａｃｓとを用いて、

Ｔ１≦（Ｔａｃｓ－Ｔｌａｓｔ）＋ε≦Ｔ２

を満たすか否かを判定する。ここで、定数εは、上述したように、電子機器１０と認証装置３０との間でのパケットの受け渡しに要する時間や、電子機器１０の内部での処理時間等を吸収する固定値である。また、ここでの更新時刻情報Ｔｌａｓｔは、最後に先に図１１に示したステップＳ１４２及びステップＳ１４３にて新たな公開鍵データPK_{Mnew}をリポジトリに記憶させて更新した時刻を示すものとする。いずれにせよ、認証装置３０は、この更新時刻情報Ｔｌａｓｔをリポジトリ等に記憶している必要がある。さらに、アクセス時刻情報Ｔａｃｓは、このステップＳ１８８における時刻を示すものとする。

【０１４０】データ送受信システムにおいては、Ｔ１≦（Ｔａｃｓ－Ｔｌａｓｔ）＋ε≦Ｔ２を満たさないものと判定された場合には、認証装置３０は、電子機器１０の公開鍵データPK_Mを用いて、鍵データの更新のリクエストを拒否する旨を示す検証結果情報としての警告情報MSG_{alert}を暗号化し、暗号化警告情報Ｅ（PK_M，MSG_{alert}）を生成するとともに、認証機関ＣＡの秘密鍵データSK_{CA}を用いて暗号化警告情報Ｅ（PK_M，MSG_{alert}）の電子署名Ｓｉｇを生成し、ステップＳ１８９において、レスポンスとして、生成した暗号化警告情報Ｅ（PK_M，MSG_{alert}）と、この暗号化警告情報Ｅ（PK_M，MSG_{alert}）に対する電子署名Ｓｉｇとを、電子機器１０に対して送信する。

【０１４１】一方、データ送受信システムにおいては、Ｔ１≦（Ｔａｃｓ－Ｔｌａｓｔ）＋ε≦Ｔ２を満たすものと判定された場合には、認証装置３０は、電子機器１０の公開鍵データPK_Mを用いて、鍵データの更新のリクエストを受諾する旨を示す検証結果情報としての受諾情報MSG_{OK}を暗号化し、暗号化受諾情報Ｅ（PK_M，MSG_{OK}）を生成するとともに、認証機関ＣＡの秘密鍵データSK_{CA}を用いて暗号化受諾情報Ｅ（PK_M，MSG_{OK}）の電子署名Ｓｉｇを生成し、ステップＳ１９０において、レスポンスとして、生成した暗号化受諾情報Ｅ（PK_M，MSG_{OK}）と、この暗号化受諾情報Ｅ（PK_M，MSG_{OK}）に対する電子署名Ｓｉｇとを、電子機器１０に対して送信する。

【０１４２】データ送受信システムにおいては、ステップＳ１９１において、電子機器１０は、認証装置３０から暗号化警告情報Ｅ（PK_M，MSG_{alert}）及び電子署名Ｓｉｇを受信すると、ステップＳ１９２において、ＣＰＵ１１の制御のもとに、電子署名Ｓｉｇの検証

を行うことによって暗号化警告情報Ｅ（PK_M，ＭＳＧａｌｅｒｔ）の検証を行う。

【０１４３】データ送受信システムにおいては、電子機器１０による暗号化警告情報Ｅ（PK_M，ＭＳＧａｌｅｒｔ）の検証の結果、暗号化警告情報Ｅ（PK_M，MSG_{alert}）が不当なものであると判定された場合には、ステップＳ１９３において、電子機器１０は、警告として、暗号化警告情報エラーを示す制御信号を通信部１８を介して認証装置３０に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化警告情報エラーを示す制御信号を認証装置３０が受信すると、認証装置３０は、エラー終了する。

【０１４４】一方、データ送受信システムにおいては、電子機器１０による暗号化警告情報Ｅ（PK_M，ＭＳＧａｌｅｒｔ）の検証の結果、暗号化警告情報Ｅ（PK_M，MSG_{alert}）が正当なものであると判定された場合には、複製機器が存在していることを示すことから、ステップＳ１９３において、電子機器１０は、警告を発し、認証装置３０に対してその旨を通知するとともに、複製機器に対抗するための上述したような所定の処理へと移行する。

【０１４５】また、データ送受信システムにおいては、ステップＳ１９４において、電子機器１０は、認証装置３０から暗号化受諾情報Ｅ（PK_M，MSG_{OK}）及び電子署名Ｓｉｇを受信すると、ステップＳ１９５において、ＣＰＵ１１の制御のもとに、電子署名Ｓｉｇの検証を行うことによって暗号化受諾情報Ｅ（PK_M，ＭＳＧＯＫ）の検証を行う。

【０１４６】データ送受信システムにおいては、電子機器１０による暗号化受諾情報Ｅ（PK_M，MSG_{OK}）の検証の結果、暗号化受諾情報Ｅ（PK_M，MSG_{OK}）が不当なものであると判定された場合には、ステップＳ１９３において、電子機器１０は、警告として、暗号化受諾情報エラーを示す制御信号を通信部１８を介して認証装置３０に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化受諾情報エラーを示す制御信号を認証装置３０が受信すると、認証装置３０は、エラー終了する。

【０１４７】一方、データ送受信システムにおいては、電子機器１０による暗号化受諾情報Ｅ（PK_M，ＭＳＧＯＫ）の検証の結果、暗号化受諾情報Ｅ（PK_M，MSG_{OK}）が正当なものであると判定された場合には、複製機器が存在していないことを示すことから、ステップＳ１９６において、電子機器１０は、鍵データの更新処理へと移行し、先に図１０に示した更新処理のプロトコルにしたがって、先に図１１に示したような処理を行い、認証装置３０に対する公開鍵データの更新を行う。

【０１４８】このように、データ送受信システムは、鍵データの更新間隔の整合性の検証を認証装置３０の側で行うことによっても、複製機器を追跡してその存在を検出することができる。

【０１４９】最後に、鍵データの更新間隔の整合性の検証を電子機器１０及び認証装置３０の両者によって行う場合について、図１６を用いて説明する。

【０１５０】データ送受信システムにおいては、同図に示すように、ステップＳ２０１において、電子機器１０は、ＣＰＵ１１の制御のもとに、上述したタイマーが計数するタイマー値が"０"であるか否かを判定する。データ送受信システムにおいては、タイマー値が"０"でないものと判定された場合には、ステップＳ２０２において、電子機器１０は、ＣＰＵ１１の制御のもとに、タイマー値を"１"だけデクリメントさせ、タイマー値が"０"であるか否かを再度判定する。

【０１５１】そして、データ送受信システムにおいては、電子機器１０は、このような処理をタイマー値が"０"となるまで繰り返し、タイマー値が"０"であるものと判定された場合には、ステップＳ２０３において、ＣＰＵ１１の制御のもとに、乱数発生部１５によって乱数値ｔを発生し、ステップＳ２０４において、ＣＰＵ１１の制御のもとに、この乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たすか否かを判定する。データ送受信システムにおいては、電子機器１０は、乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たさない場合には、ステップＳ２０３からの処理を繰り返し、発生した乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たすまで、乱数値ｔを発生する。

【０１５２】データ送受信システムにおいては、電子機器１０は、乱数値ｔが所定の範囲$T_1 \leqq t \leqq T_2$を満たす場合には、ステップＳ２０５において、ＣＰＵ１１の制御のもとに、この乱数値ｔを次回の鍵データの更新までの時間ｔｉｍｅｒ＿ｎとしてＥＥＰＲＯＭ１４等に記憶させる。

【０１５３】これと同時に、データ送受信システムにおいては、ステップＳ２０６において、電子機器１０は、認証装置３０に対して、ＣＰＵ１１の制御のもとに、最後に鍵データを更新した時刻を示す更新時刻情報Ｔｌａｓｔのリクエストを行う旨の所定の制御信号と、鍵データの更新のリクエストを行う旨の所定の制御信号とを通信部１８を介して送信する。なお、ここでの更新時刻情報Ｔｌａｓｔは、上述したように、最後に先に図１１に示したステップＳ１４２及びステップＳ１４３にて新たな公開鍵データPK_{Mnew}をリポジトリに記憶させて更新した時刻を示すものとする。いずれにせよ、認証装置３０は、この更新時刻情報Ｔｌａｓｔをリポジトリ等に記憶している必要がある。

【０１５４】以後、データ送受信システムにおいては、電子機器１０による鍵データの更新間隔の整合性の検証と、認証装置３０による鍵データの更新間隔の整合性の検証とを並列的に行う。

【０１５５】データ送受信システムにおいては、ステッ

プＳ２０７において、認証装置３０は、リクエストを受信すると、電子機器１０の公開鍵データPK_Mを用いてリクエストされた更新時刻情報Ｔｌａｓｔを暗号化し、暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）を生成するとともに、認証機関ＣＡの秘密鍵データSK_{CA}を用いて暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）の電子署名Ｓｉｇを生成し、ステップＳ２０８において、レスポンスとして、生成した暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）と、この暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）に対する電子署名Ｓｉｇとを、電子機器１０に対して送信する。また、データ送受信システムにおいては、ステップＳ２０９において、認証装置３０は、更新時刻情報Ｔｌａｓｔと、電子機器１０によってアクセスされた時刻を示すアクセス時刻情報Ｔａｃｓとを用いて、

$T_1 \leqq (T_{acs} - T_{last}) + \varepsilon \leqq T_2$

を満たすか否かを判定する。ここで、定数εは、上述したように、電子機器１０と認証装置３０との間でのパケットの受け渡しに要する時間や、電子機器１０の内部での処理時間等を吸収する固定値である。また、アクセス時刻情報Ｔａｃｓは、このステップＳ２０９における時刻を示すものとする。

【０１５６】データ送受信システムにおいては、$T_1 \leqq (T_{acs} - T_{last}) + \varepsilon \leqq T_2$を満たすものと判定された場合には、認証装置３０は、電子機器１０の公開鍵データPK_Mを用いて、鍵データの更新のリクエストを受諾する旨を示す検証結果情報としての受諾情報MSG_{OK}を暗号化し、暗号化受諾情報Ｅ（PK_M，MSG_{OK}）を生成するとともに、認証機関ＣＡの秘密鍵データSK_{CA}を用いて暗号化受諾情報Ｅ（PK_M，MSG_{OK}）の電子署名Ｓｉｇを生成し、ステップＳ２１０において、レスポンスとして、生成した暗号化受諾情報Ｅ（PK_M，MSG_{OK}）と、この暗号化受諾情報Ｅ（PK_M，MSG_{OK}）に対する電子署名Ｓｉｇとを、電子機器１０に対して送信する。

【０１５７】一方、データ送受信システムにおいては、$T_1 \leqq (T_{acs} - T_{last}) + \varepsilon \leqq T_2$を満たさないものと判定された場合には、認証装置３０は、電子機器１０の公開鍵データPK_Mを用いて、鍵データの更新のリクエストを拒否する旨を示す検証結果情報としての警告情報MSG_{alert}を暗号化し、暗号化警告情報Ｅ（PK_M，MSG_{alert}）を生成するとともに、認証機関ＣＡの秘密鍵データSK_{CA}を用いて暗号化警告情報Ｅ（PK_M，MSG_{alert}）の電子署名Ｓｉｇを生成し、ステップＳ２１１において、レスポンスとして、生成した暗号化警告情報Ｅ（PK_M，MSG_{alert}）と、この暗号化警告情報Ｅ（PK_M，MSG_{alert}）に対する電子署名Ｓｉｇとを、電子機器１０に対して送信する。

【０１５８】データ送受信システムにおいては、ステップＳ２１２において、電子機器１０は、認証装置３０から暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）及び電子署名Ｓｉｇを受信すると、ステップＳ２１３において、ＣＰＵ１１の制御のもとに、電子署名Ｓｉｇの検証を行うことによって暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）の検証を行う。

【０１５９】データ送受信システムにおいては、電子機器１０による暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）の検証の結果、暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）が不当なものであると判定された場合には、ステップＳ２２０において、電子機器１０は、警告として、暗号化更新時刻情報エラーを示す制御信号を通信部１８を介して認証装置３０に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化更新時刻情報エラーを示す制御信号を認証装置３０が受信すると、認証装置３０は、エラー終了する。

【０１６０】一方、データ送受信システムにおいては、電子機器１０による暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）の検証の結果、暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）が正当なものであると判定された場合には、ステップＳ２１４において、電子機器１０は、ＣＰＵ１１の制御のもとに、現在時刻を示す現在時刻情報Ｔｎｏｗと、暗号化／復号部１７によって暗号化更新時刻情報Ｅ（PK_M，Ｔｌａｓｔ）を復号して得られた更新時刻情報Ｔｌａｓｔと、上述した前回のタイマー値ｔｉｍｅｒとに基づいて、

$T_{now} - (T_{last} + timer) \leqq \varepsilon$

を満たすか否かを判定する。なお、現在時刻情報Ｔｎｏｗは、このステップＳ２１４における時刻を示すものとする。

【０１６１】データ送受信システムにおいては、$T_{now} - (T_{last} + timer) \leqq \varepsilon$を満たすものと判定された場合には、複製機器が存在していないことを示すことから、ステップＳ２１７において、電子機器１０は、鍵データの更新処理へと移行し、先に図１０に示した更新処理のプロトコルにしたがって、先に図１１に示したような処理を行い、認証装置３０に対する公開鍵データの更新を行う。

【０１６２】一方、データ送受信システムにおいては、$T_{now} - (T_{last} + timer) \leqq \varepsilon$を満たさないものと判定された場合には、複製機器が存在していることを示すことから、ステップＳ２２０において、電子機器１０は、警告を発し、認証装置３０に対してその旨を通知するとともに、複製機器に対抗するための上述したような所定の処理へと移行する。

【０１６３】また、データ送受信システムにおいては、ステップＳ２１５において、電子機器１０は、認証装置３０から暗号化受諾情報Ｅ（PK_M，MSG_{OK}）及び電子署名Ｓｉｇを受信すると、ステップＳ２１６におい

て、ＣＰＵ１１の制御のもとに、電子署名Ｓｉｇの検証を行うことによって暗号化受諾情報Ｅ（PK_M，ＭＳＧＯＫ）の検証を行う。

【０１６４】データ送受信システムにおいては、電子機器１０による暗号化受諾情報Ｅ（PK_M，MSG_{OK}）の検証の結果、暗号化受諾情報Ｅ（PK_M，MSG_{OK}）が不当なものであると判定された場合には、ステップＳ２２０において、電子機器１０は、警告として、暗号化受諾情報エラーを示す制御信号を通信部１８を介して認証装置３０に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化受諾情報エラーを示す制御信号を認証装置３０が受信すると、認証装置３０は、エラー終了する。

【０１６５】一方、データ送受信システムにおいては、電子機器１０による暗号化受諾情報Ｅ（PK_M，ＭＳＧＯＫ）の検証の結果、暗号化受諾情報Ｅ（PK_M，MSG_{OK}）が正当なものであると判定された場合には、複製機器が存在していないことを示すことから、ステップＳ２１７において、電子機器１０は、鍵データの更新処理へと移行し、先に図１０に示した更新処理のプロトコルにしたがって、先に図１１に示したような処理を行い、認証装置３０に対する公開鍵データの更新を行う。

【０１６６】さらに、データ送受信システムにおいては、ステップＳ２１８において、電子機器１０は、認証装置３０から暗号化警告情報Ｅ（PK_M，ＭＳＧａｌｅｒｔ）及び電子署名Ｓｉｇを受信すると、ステップＳ２１９において、ＣＰＵ１１の制御のもとに、電子署名Ｓｉｇの検証を行うことによって暗号化警告情報Ｅ（PK_M，MSG_{alert}）の検証を行う。

【０１６７】データ送受信システムにおいては、電子機器１０による暗号化警告情報Ｅ（PK_M，ＭＳＧａｌｅｒｔ）の検証の結果、暗号化警告情報Ｅ（PK_M，MSG_{alert}）が不当なものであると判定された場合には、ステップＳ２２０において、電子機器１０は、警告として、暗号化警告情報エラーを示す制御信号を通信部１８を介して認証装置３０に対して送信し、エラー終了する。これに応じて、データ送受信システムにおいては、暗号化警告情報エラーを示す制御信号を認証装置３０が受信すると、認証装置３０は、エラー終了する。

【０１６８】一方、データ送受信システムにおいては、電子機器１０による暗号化警告情報Ｅ（PK_M，ＭＳＧａｌｅｒｔ）の検証の結果、暗号化警告情報Ｅ（PK_M，MSG_{alert}）が正当なものであると判定された場合には、複製機器が存在していることを示すことから、ステップＳ２２０において、電子機器１０は、警告を発し、認証装置３０に対してその旨を通知するとともに、複製機器に対抗するための上述したような所定の処理へと移行する。

【０１６９】このように、データ送受信システムは、鍵データの更新間隔の整合性の検証を電子機器１０及び認証装置３０の両者で行うことによっても、複製機器を追跡してその存在を検出することができる。

【０１７０】なお、ここでは、電子機器１０による鍵データの更新間隔の整合性の検証結果と、認証装置３０による鍵データの更新間隔の整合性の検証結果とが同一であるか否かにかかわらず、各検証結果に応じて公開鍵データの更新を行うか警告を発するかを決定しているが、データ送受信システムにおいては、より厳密には、各検証結果の組み合わせに応じて以後の処理を決定するのが望ましい。

【０１７１】具体的には、検証結果の組み合わせとしては、電子機器１０による検証結果及び認証装置３０による検証結果の両者が正当、すなわち、複製機器が存在していないことを示す結果である場合、電子機器１０による検証結果は正当であるものの、認証装置３０による検証結果が不当、すなわち、複製機器が存在していることを示す結果である場合、認証装置３０による検証結果は正当であるものの、電子機器１０による検証結果が不当である場合、及び電子機器１０による検証結果及び認証装置３０による検証結果の両者が不当である場合の４つのケースが想定される。

【０１７２】そこで、データ送受信システムにおいては、電子機器１０による検証結果及び認証装置３０による検証結果の両者が正当である場合には、複製機器が確実に存在していないものとして、公開鍵データの更新処理へと移行し、電子機器１０による検証結果及び認証装置３０による検証結果の両者が不当である場合には、複製機器が確実に存在しているものとして、複製機器に対抗するための上述したような所定の処理へと移行する。

【０１７３】一方、データ送受信システムにおいては、電子機器１０による検証結果と認証装置３０による検証結果とが異なるものである場合には、図１６に示す処理を再度行うか、複製機器が存在している可能性がある旨を結果として判定するか、一方でも不当であれば不当として複製機器に対抗するための上述したような所定の処理へと移行するか、又は今回は正当であるものとし、次回の検証の際に今回の結果を反映させ、判断を繰り越すといった処理を行うことができる。

【０１７４】このように、データ送受信システムは、鍵データの更新間隔の整合性の検証を行うことにより、複製機器を追跡してその存在を検出することができる。この際、データ送受信システムにおいては、電子機器１０又は複製機器と認証装置３０との間で行われる通信によって得られる上述した各種情報を用いた総合的な判断を行うことにより、複製機器の存在の検出のみならず、複製機器の割り出しを行うことも可能となる。

【０１７５】以上説明したように、データ送受信システムは、従来の共通鍵暗号方式に基づく機器間認証を行うことなく、公開鍵暗号方式に基づく機器間認証を行うこ

とができ、鍵データの更新間隔の整合性を検証することにより、不完全な複製機器が接続された場合のみならず、完全な複製機器が接続された場合であっても、複製機器を追跡し、複製機器の存在を検出することができる。

【０１７６】これにより、データ送受信システムにおいては、複製機器をネットワークから排除することができることから、上述した機器間認証によって認証された電子機器は、信頼できるものとなる。このとき、データ送受信システムにおいては、信頼できる電子機器間は、信頼できるパス（trusted path）が張られている状態となる。データ送受信システムにおいては、この信頼できる電子機器に対して新たな電子機器が接続された場合には、信頼できる電子機器と新たに接続された電子機器との間で機器間認証を行う。データ送受信システムにおいては、この機器間認証によって新たに接続された電子機器が正当なものであると認証された場合には、新たに信頼できるパスが形成される。データ送受信システムにおいては、このような手順が繰り返し行われることにより、信頼できるネットワーク（trusted network）が形成される。なお、データ送受信システムにおいては、この信頼できるネットワークを信頼できないネットワーク内に形成することが可能である。

【０１７７】なお、本発明は、上述した実施の形態に限定されるものではない。例えば、上述した実施の形態では、電子機器１０，２０と認証装置３０との間で行われる通信の際に、各種通信内容を暗号化するといったように、通信内容を保護する機構を設けるものとして説明したが、本発明は、いわゆるＩＰｖ６（Internet Protocol Version 6）を完全にサポートしている環境に適用された場合には、ＩＰｖ６の必須機能であるＩＰｓｅｃ（IP Security）を用いることによって通信内容の保護が可能となることから、上述した通信内容を保護する機構を省略することが可能となる。

【０１７８】また、本発明は、上述した機器固有情報を機種毎に体系的に定めるものとした場合には、上述した信頼できるネットワーク上でのサービス内容を制限することが可能となる。

【０１７９】さらに、上述した実施の形態では、先に図１４乃至図１６に示した更新時刻情報Ｔｌａｓｔが最後に先に図１１に示したステップＳ１４２及びステップＳ１４３にて新たな公開鍵データＰＫＭｎｅｗをリポジトリに記憶させて更新した時刻を示すものとし、先に図１４又は図１６に示した現在時刻情報Ｔｎｏｗ及び先に図１５又は図１６に示したアクセス時刻情報Ｔａｃｓが判定の際の時刻を示すものとして説明したが、本発明は、各時刻情報を必ずしもこのように定義する必要はない。すなわち、電子機器１０が鍵データの更新間隔の整合性の検証を主に行う場合の各時刻情報は、電子機器１０が行う一連の処理のうち所定の工程での時刻を比較できるものであればよく、認証装置３０が鍵データの更新間隔の整合性の検証を主に行う場合の各時刻情報は、認証装置３０が行う一連の処理のうち所定の工程での時刻を比較できるものであればよい。したがって、本発明は、各時刻情報として、種々のバリエーションを考えることができるものである。

【０１８０】さらにまた、本発明は、先に図１６に示したように、電子機器１０と認証装置３０とが協調して動作する場合には、各時刻情報の全てを電子機器１０が行う一連の処理のうち所定の工程での時刻を示すものとし、鍵データの更新間隔の整合性の検証については認証装置３０が行うといったように、各時刻情報の取得とこれらの時刻情報を用いた鍵データの更新間隔の整合性の検証とを電子機器１０と認証装置３０とに振り分けることもできる。この場合、本発明においては、リクエストに際して暗号化した時刻情報を併せて送信するようにすればよい。

【０１８１】また、上述した実施の形態では、２つの電子機器１０，２０が接続された環境であるものとし、また、電子機器１０の複製機器が存在する場合について説明したが、本発明は、少なくとも２つ以上の電子機器が相互に接続された環境にも容易に適用することができ、また、任意の電子機器の複製機器が複数存在する場合についても容易に適用することができる。

【０１８２】このように、本発明は、その趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

【０１８３】

【発明の効果】以上詳細に説明したように、本発明にかかる電子機器は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する電子機器であって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、最後に公開鍵データを更新した時刻を示す更新時刻情報を認証装置から取得する取得手段と、現在時刻を示す現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備える。

【０１８４】したがって、本発明にかかる電子機器は、現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、更新間隔検証手段によって公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することができ、複製機器をネットワークから排除することができ

る。

【０１８５】また、本発明にかかる認証装置は、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置であって、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、この更新間隔検証手段による検証の結果に応じた検証結果情報を電子機器に対して送信する送信手段とを備える。

【０１８６】したがって、本発明にかかる認証装置は、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを更新間隔検証手段によって検証し、公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することが可能となり、複製機器をネットワークから排除することが可能となる。

【０１８７】さらに、本発明にかかる複製機器検出システムは、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、電子機器は、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、最後に公開鍵データを更新した時刻を示す更新時刻情報を認証装置から取得する取得手段と、現在時刻を示す現在時刻情報と、取得手段によって取得した更新時刻情報と、乱数発生手段によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備える。

【０１８８】したがって、本発明にかかる複製機器検出システムは、現在時刻情報と、電子機器によって取得した更新時刻情報と、電子機器によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することができ、複製機器をネットワークから排除することができる。

【０１８９】さらにまた、本発明にかかる複製機器検出方法は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する電子機器による公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を電子機器によって発生する乱数発生工程と、最後に公開鍵データを更新した時刻を示す更新時刻情報を電子機器によって認証装置から取得する取得工程と、現在時刻を示す現在時刻情報と、取得工程にて取得した更新時刻情報と、乱数発生工程にて前回の公開鍵データの更新時に発生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証する更新間隔検証工程とを備える。

【０１９０】したがって、本発明にかかる複製機器検出方法は、現在時刻情報と、電子機器によって取得した更新時刻情報と、電子機器によって前回の公開鍵データの更新時に発生した乱数値とに基づいて、電子機器によって公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することが可能となり、複製機器をネットワークから排除することが可能となる。

【０１９１】また、本発明にかかる複製機器検出システムは、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置は、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、この更新間隔検証手段による検証の結果に応じた検証結果情報を電子機器に対して送信する送信手段とを備える。

【０１９２】したがって、本発明にかかる複製機器検出システムは、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することができ、複製機器をネットワークから排除することができる。

【０１９３】さらに、本発明にかかる複製機器検出方法は、正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である

複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、所定のネットワークを介して接続されている正当な電子機器と正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証する更新間隔検証工程と、この更新間隔検証工程による検証の結果に応じた検証結果情報を認証装置から電子機器に対して送信する送信工程とを備える。

【０１９４】したがって、本発明にかかる複製機器検出方法は、アクセス時刻情報と更新時刻情報との差分が所定の範囲内にあるか否かを認証装置によって検証し、公開鍵データの更新間隔の整合性を検証することにより、複製機器を追跡してその存在を検出することが可能となり、複製機器をネットワークから排除することが可能となる。

【図面の簡単な説明】

【図１】本発明の実施の形態として示すデータ送受信システムの構成を説明するブロック図である。

【図２】同データ送受信システムを構成する電子機器の構成を説明するブロック図である。

【図３】同データ送受信システムにおける通信プロトコルを説明する図であって、同電子機器から認証機関に対して公開鍵データを登録する際の同電子機器と同認証機関における認証装置との間の通信プロトコルを説明する図である。

【図４】同データ送受信システムにおいて同電子機器から同認証機関に対して公開鍵データを登録する際の一連の処理を説明するフローチャートである。

【図５】同データ送受信システムにおける通信プロトコルを説明する図であって、２つの電子機器の間で機器間認証を行う際の同電子機器と同認証装置との間の通信プロトコルを説明する図である。

【図６】同データ送受信システムにおいて２つの電子機器の間で機器間認証を行う際の第１の処理としての一連の処理を説明するフローチャートである。

【図７】同データ送受信システムにおいて２つの電子機器の間で機器間認証を行う際の第２の処理としての一連の処理を説明するフローチャートである。

【図８】同データ送受信システムにおいて２つの電子機器の間で機器間認証を行う際の第３の処理としての一連の処理を説明するフローチャートである。

【図９】同データ送受信システムにおいて２つの電子機器の間で機器間認証を行う際の第４の処理としての一連の処理を説明するフローチャートである。

【図１０】同データ送受信システムにおける通信プロトコルを説明する図であって、同電子機器から同認証機関に対して登録又は更新された公開鍵データの更新を行う際の同電子機器と同認証装置との間の通信プロトコルを説明する図である。

【図１１】同データ送受信システムにおいて同電子機器から同認証機関に対して登録又は更新された公開鍵データの更新を行う際の一連の処理を説明するフローチャートである。

【図１２】同データ送受信システムにおいて同電子機器から同認証機関に対して登録又は更新された公開鍵データの更新を行うにあたって行われる動作の概念を説明するフローチャートである。

【図１３】同データ送受信システムにおける公開鍵データの更新間隔のタイミングを説明する図であって、（Ａ）は、正当な機器である同電子機器から同認証装置に対して更新のリクエストを通知するタイミングを示し、（Ｂ）は、複製機器から同認証装置に対して更新のリクエストを通知するタイミングを示し、（Ｃ）は、同認証装置に対してリクエストの通知が到達する間隔を示す図である。

【図１４】同データ送受信システムにおいて複製機器を追跡し、その存在を検出する際の一連の処理を説明するフローチャートであって、鍵データの更新間隔の整合性の検証を同電子機器によって行う場合について説明する図である。

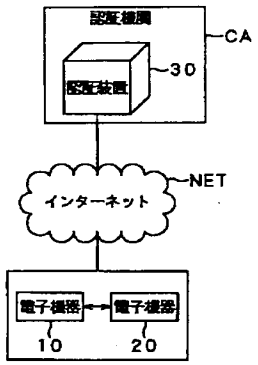
【図１５】同データ送受信システムにおいて複製機器を追跡し、その存在を検出する際の一連の処理を説明するフローチャートであって、鍵データの更新間隔の整合性の検証を同認証装置によって行う場合について説明する図である。

【図１６】同データ送受信システムにおいて複製機器を追跡し、その存在を検出する際の一連の処理を説明するフローチャートであって、鍵データの更新間隔の整合性の検証を同電子機器及び同認証装置の両者によって行う場合について説明する図である。

【符号の説明】

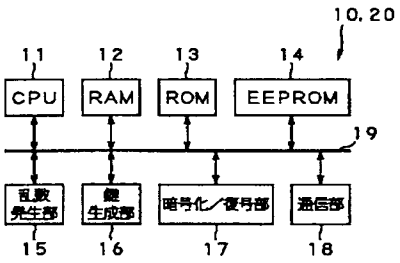
１０，２０　電子機器、　１１　ＣＰＵ、　１２　ＲＡＭ、　１３　ＲＯＭ、１４　ＥＥＰＲＯＭ、　１５　乱数発生部、　１６　鍵生成部、　１７　暗号化／復号部、　１８　通信部、　３０　認証装置、　ＣＡ　認証機関

【図１】



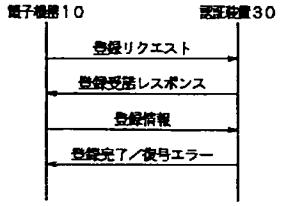
データ送受信システムの構成ブロック図

【図２】



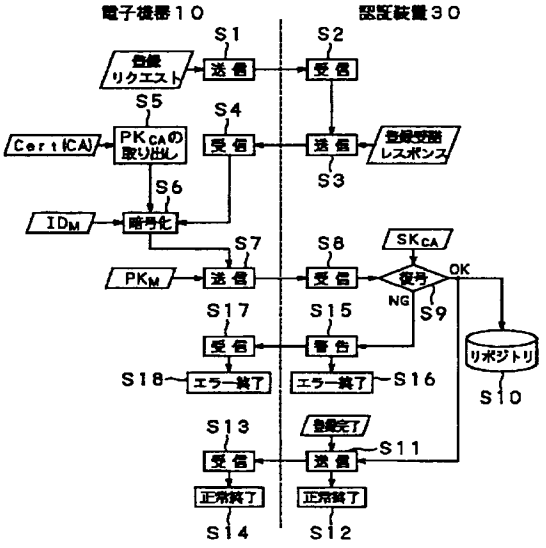
電子機器の構成ブロック図

【図３】



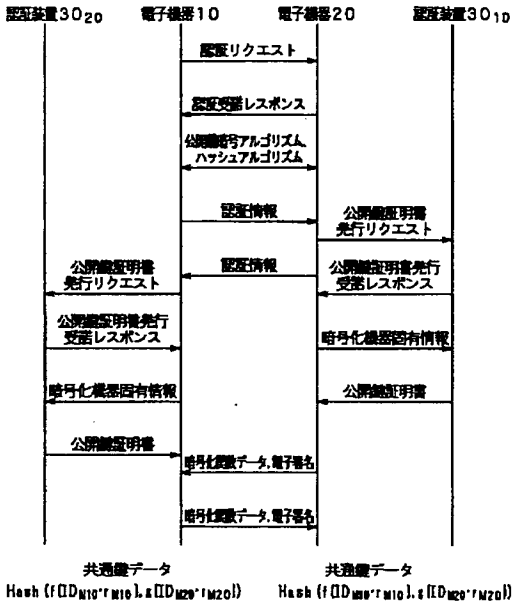
データ送受信システムにおける通信プロトコルの説明図

【図４】



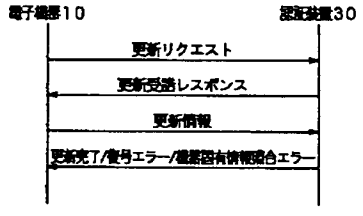
データ送受信システムにおける一連の処理工程

【図５】



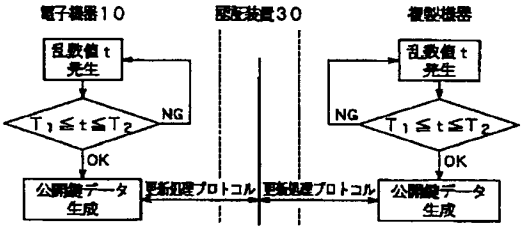
データ送受信システムにおける通信プロトコルの説明図

【図１０】



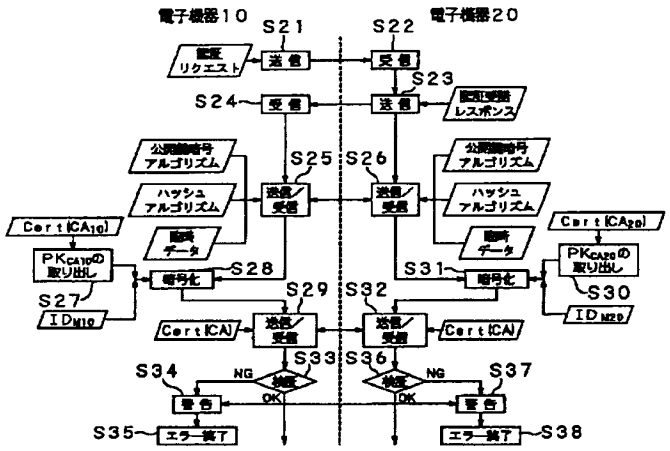
データ送受信システムにおける通信プロトコルの説明図

【図１２】



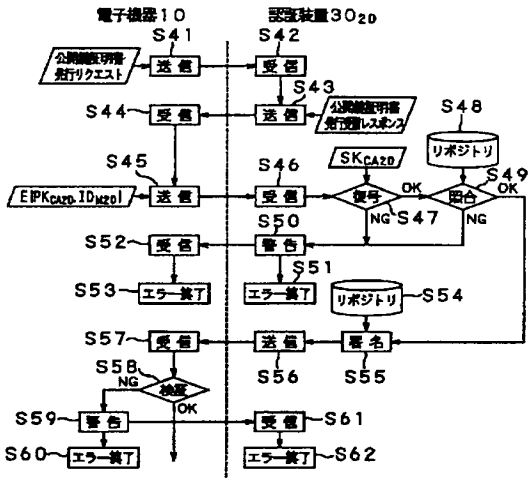
データ送受信システムにおける一連の処理工程

【図６】



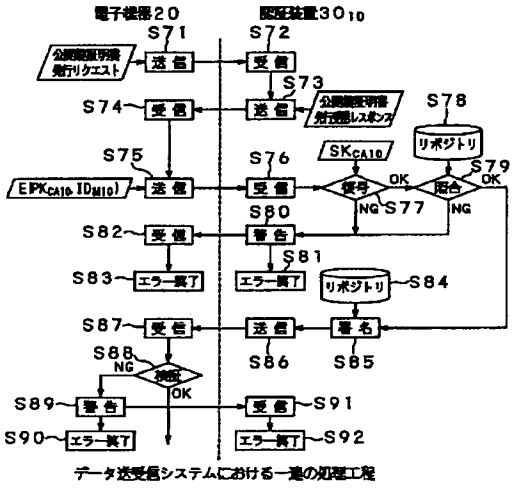
データ送受信システムにおける一連の処理工程

【図７】



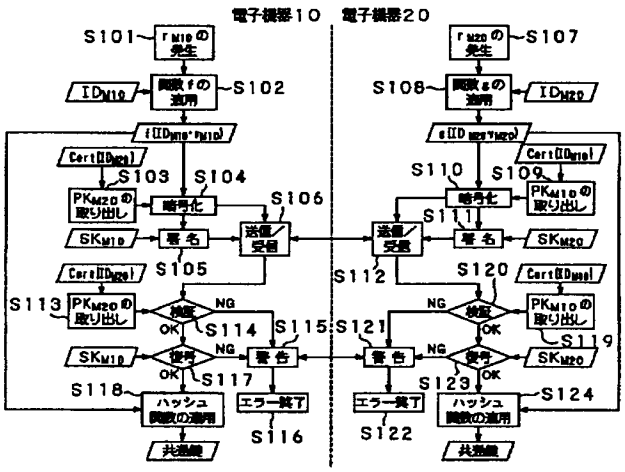
データ送受信システムにおける一連の処理工程

【図８】



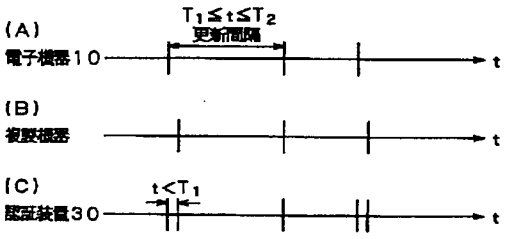
データ送受信システムにおける一連の処理工程

【図９】



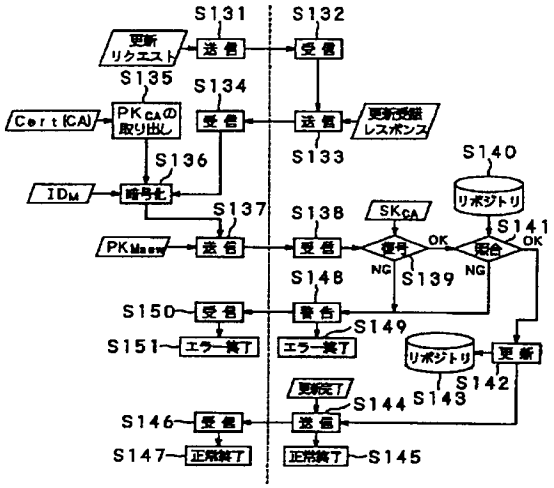
データ送受信システムにおける一連の処理工程

【図１３】



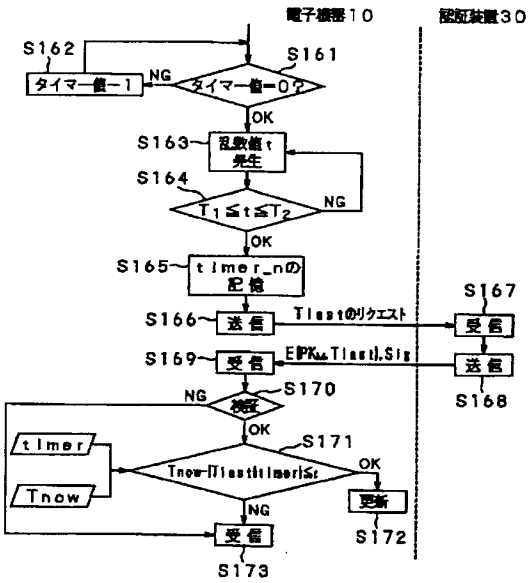
データ送受信システムにおける更新間隔のタイミングの説明図

【図１１】



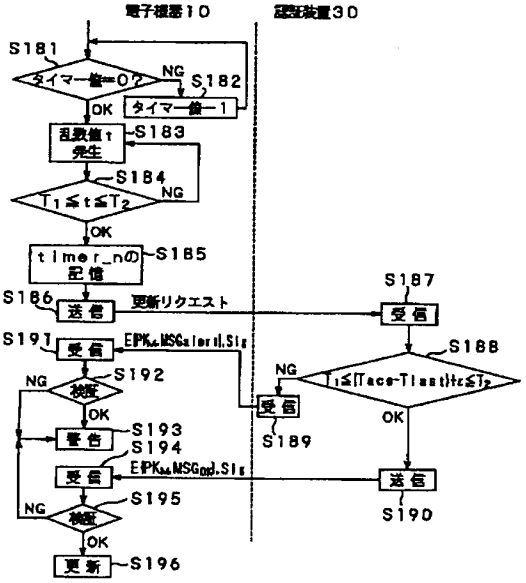
データ送受信システムにおける一連の処理工程

【図１４】



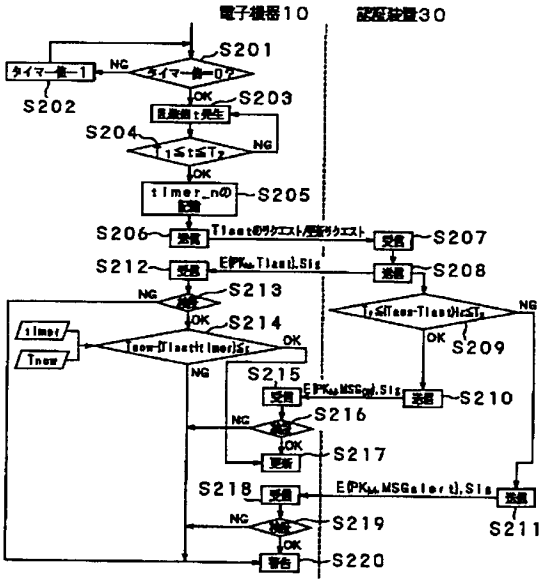
データ送受信システムにおける一連の処理工程

【図１５】



データ送受信システムにおける一連の処理工程

【図１６】



データ送受信システムにおける一連の処理工程

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成17年7月21日(2005.7.21)

【公開番号】特開2003-163661(P2003-163661A)
【公開日】平成15年6月6日(2003.6.6)
【出願番号】特願2001-361032(P2001-361032)
【国際特許分類第７版】
　Ｈ０４Ｌ　9/10
　Ｇ０９Ｃ　1/00
　Ｈ０４Ｌ　9/32
【ＦＩ】
　Ｈ０４Ｌ　9/00　６２１Ａ
　Ｇ０９Ｃ　1/00　６４０Ｅ
　Ｈ０４Ｌ　9/00　６７５Ｄ
　Ｈ０４Ｌ　9/00　６７５Ｂ

【手続補正書】
【提出日】平成16年11月29日(2004.11.29)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する電子機器であって、
公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、
最後に公開鍵データを更新した時刻を示す更新時刻情報を上記認証装置から取得する取得手段と、
現在時刻を示す現在時刻情報と、上記取得手段によって取得した上記更新時刻情報と、上記乱数発生手段によって前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えること
を特徴とする電子機器。
【請求項２】
上記乱数発生手段によって発生した上記乱数値を、次回の公開鍵データの更新までの時間として記憶する記憶手段を備えること
を特徴とする請求項１記載の電子機器。
【請求項３】
公開鍵暗号方式における復号を行う復号手段を備え、
上記取得手段は、上記認証装置によって上記更新時刻情報が暗号化された暗号化更新時刻情報を取得し、
上記復号手段は、上記暗号化更新時刻情報を復号し、上記更新時刻情報を得ること
を特徴とする請求項１記載の電子機器。
【請求項４】
上記暗号化更新時刻情報に対する上記認証装置の電子署名の検証を行い、上記暗号化更

新時刻情報の検証を行う更新時刻情報検証手段を備えること
を特徴とする請求項３記載の電子機器。
【請求項５】
上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が不当なものであると判定された場合に、警告としての暗号化更新時刻情報エラーを示す制御信号を上記認証装置に対して送信する送信手段を備えること
を特徴とする請求項４記載の電子機器。
【請求項６】
上記更新間隔検証手段は、上記更新時刻情報検証手段による上記暗号化更新時刻情報の検証の結果、上記暗号化更新時刻情報が正当なものであると判定された場合に、上記公開鍵データの更新間隔の整合性の検証を行うこと
を特徴とする請求項４記載の電子機器。
【請求項７】
公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置であって、
所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、
上記更新間隔検証手段による検証の結果に応じた検証結果情報を上記電子機器に対して送信する送信手段とを備えること
を特徴とする認証装置。
【請求項８】
上記検証結果情報を上記正当な電子機器の公開鍵データを用いて暗号化する暗号化手段を備え、
上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報を上記電子機器に対して送信すること
を特徴とする請求項７記載の認証装置。
【請求項９】
上記認証機関の秘密鍵データを用いて上記検証結果情報の電子署名を生成する電子署名生成手段を備え、
上記送信手段は、上記暗号化手段によって暗号化された上記検証結果情報と上記電子署名とを上記電子機器に対して送信すること
を特徴とする請求項８記載の認証装置。
【請求項１０】
正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、
上記電子機器は、
公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を発生する乱数発生手段と、
最後に公開鍵データを更新した時刻を示す更新時刻情報を上記認証装置から取得する取得手段と、
現在時刻を示す現在時刻情報と、上記取得手段によって取得した上記更新時刻情報と、上記乱数発生手段によって前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段とを備えること
を特徴とする複製機器検出システム。

【請求項１１】
正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、
公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する上記電子機器による公開鍵データの更新間隔として予め規定された所定の範囲内の乱数値を上記電子機器によって発生する乱数発生工程と、
最後に公開鍵データを更新した時刻を示す更新時刻情報を上記電子機器によって上記認証装置から取得する取得工程と、
現在時刻を示す現在時刻情報と、上記取得工程にて取得した上記更新時刻情報と、上記乱数発生工程にて前回の公開鍵データの更新時に発生した上記乱数値とに基づいて、上記電子機器によって上記公開鍵データの更新間隔の整合性を検証する更新間隔検証工程とを備えること
を特徴とする複製機器検出方法。
【請求項１２】
正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出システムであって、
公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置は、
所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証手段と、
上記更新間隔検証手段による検証の結果に応じた検証結果情報を上記電子機器に対して送信する送信手段とを備えること
を特徴とする複製機器検出システム。
【請求項１３】
正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器が所定のネットワークを介して接続されたことを検出する複製機器検出方法であって、
所定のネットワークを介して接続されている正当な電子機器と上記正当な電子機器が固有に有する各種情報の一部又は全てを複製することによって作製された電子機器である複製機器とのいずれかからの、公開鍵暗号方式における独立した所定の第三者機関であって公開鍵証明書を発行する認証機関が有する認証装置に対する公開鍵データの更新リクエストに応じて、アクセスされた時刻を示すアクセス時刻情報と最後に公開鍵データを更新した時刻を示す更新時刻情報との差分が、公開鍵データの更新間隔として予め規定された所定の範囲内にあるか否かを上記認証装置によって検証し、上記公開鍵データの更新間隔の整合性を検証する更新間隔検証工程と、
上記更新間隔検証工程による検証の結果に応じた検証結果情報を上記認証装置から上記電子機器に対して送信する送信工程とを備えること
を特徴とする複製機器検出方法。